

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN PRÜFUNG BEAUFTRAGTE BEHÖRDE

*B. Micheli*

An:

BARTH, Stephan  
Reinhard, Skuhra, Weise & Partner G  
Friedrichstrasse 31  
80801 München  
ALLEMAGNE

**Eingegangen**  
Reinhard • Skuhra • Weise

19. Dez. 2005

**PCT**

MITTEILUNG ÜBER DIE ÜBERSENDUNG  
DES INTERNATIONALEN VORLÄUFIGEN  
BERICHTS ZUR PATENTIERBARKEIT

(Regel 71.1 PCT)

Pris. 28.12.05 Erl. 28.12.05 Absendedatum  
(Tag/Monat/Jahr) 19.12.2005

Aktenzeichen des Anmelders oder Anwalts  
P17998SB/asc

## WICHTIGE MITTEILUNG

Internationales Aktenzeichen  
PCT/EP2004/010545

Internationales Anmeldedatum (Tag/Monat/Jahr)  
20.09.2004

Prioritätsdatum (Tag/Monat/Jahr)  
19.09.2003

Anmelder  
BRUNET Holding AG

1. Dem Anmelder wird mitgeteilt, daß ihm die mit der internationalen vorläufigen Prüfung beauftragte Behörde hiermit den zu der internationalen Anmeldung erstellten internationalen vorläufigen Bericht zur Patentierbarkeit, gegebenenfalls mit den dazugehörigen Anlagen, übermittelt.
2. Eine Kopie des Berichts wird - gegebenenfalls mit den dazugehörigen Anlagen - dem Internationalen Büro zur Weiterleitung an alle ausgewählten Ämter übermittelt.
3. Auf Wunsch eines ausgewählten Amtes wird das Internationale Büro eine Übersetzung des Berichts (jedoch nicht der Anlagen) ins Englische anfertigen und diesem Amt übermitteln.

### 4. ERINNERUNG

Zum Eintritt in die nationale Phase hat der Anmelder vor jedem ausgewählten Amt innerhalb von 30 Monaten ab dem Prioritätsdatum (oder in manchen Ämtern noch später) bestimmte Handlungen (Einreichung von Übersetzungen und Entrichtung nationaler Gebühren) vorzunehmen (Artikel 39 (1)) (siehe auch die durch das Internationale Büro im Formblatt PCT/IB/301 übermittelte Information).

Ist einem ausgewählten Amt eine Übersetzung der internationalen Anmeldung zu übermitteln, so muß diese Übersetzung auch Übersetzungen aller Anlagen zum internationalen vorläufigen Bericht zur Patentierbarkeit enthalten. Es ist Aufgabe des Anmelders, solche Übersetzungen anzufertigen und den betroffenen ausgewählten Ämtern direkt zuzuleiten.

Weitere Einzelheiten zu den maßgebenden Fristen und Erfordernissen der ausgewählten Ämter sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

Der Anmelder wird auf Artikel 33(5) hingewiesen, in welchem erklärt wird, daß die Kriterien für Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit, die im Artikel 33(2) bis (4) beschrieben werden, nur für die internationale vorläufige Prüfung Bedeutung haben, und daß "jeder Vertragsstaat (...) für die Entscheidung über die Patentfähigkeit der beanspruchten Erfindung in diesem Staat zusätzliche oder abweichende Merkmale aufstellen" kann (siehe auch Artikel 27(5)). Solche zusätzlichen Merkmale können z.B. Ausnahmen von der Patentierbarkeit, Erfordernisse für die Offenbarung der Erfindung sowie Klarheit und Stützung der Ansprüche betreffen.

Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde



Europäisches Patentamt - P.B. 5818 Patentlaan 2  
NL-2280 HV Rijswijk - Pays Bas  
Tel. +31 70 340 - 2040 Tx: 31 651 epo nl  
Fax: +31 70 340 - 3016

Bevollmächtigter Bediensteter

Micheli, M

Tel. +31 70 340-3606




# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

## PCT

### INTERNATIONALER VORLÄUFIGER BERICHT ÜBER DIE PATENTIERBARKEIT

(Kapitel II des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens)

Aktenzeichen des Anmelders oder Anwalts P17998SB/asc	<b>WEITERES VORGEHEN</b> siehe Formblatt PCT/PEA/416	
Internationales Aktenzeichen PCT/EP2004/010545	Internationales Anmeldedatum (Tag/Monat/Jahr) 20.09.2004	Prioritätsdatum (Tag/Monat/Jahr) 19.09.2003
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK G07F19/00		
Anmelder BRUNET Holding AG		
<p>1. Bei diesem Bericht handelt es sich um den internationalen vorläufigen Prüfungsbericht, der von der mit der internationalen vorläufigen Prüfung beauftragten Behörde nach Artikel 35 erstellt wurde und dem Anmelder gemäß Artikel 36 übermittelt wird.</p> <p>2. Dieser BERICHT umfaßt insgesamt 7 Blätter einschließlich dieses Deckblatts.</p> <p>3. Außerdem liegen dem Bericht ANLAGEN bei; diese umfassen</p> <p>a. <input checked="" type="checkbox"/> (an den Anmelder und das Internationale Büro gesandt) insgesamt 6 Blätter; dabei handelt es sich um</p> <p><input type="checkbox"/> Blätter mit der Beschreibung, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit Berichtigungen, denen die Behörde zugestimmt hat (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsvorschriften).</p> <p><input checked="" type="checkbox"/> Blätter, die frühere Blätter ersetzen, die aber aus den in Feld Nr. 1, Punkt 4 und im Zusatzfeld angegebenen Gründen nach Auffassung der Behörde eine Änderung enthalten, die über den Offenbarungsgehalt der internationalen Anmeldung in der ursprünglich eingereichten Fassung hinausgeht.</p> <p>b. <input type="checkbox"/> (nur an das Internationale Büro gesandt) insgesamt (bitte Art und Anzahl der/des elektronischen Datenträger(s) angeben), der/die ein Sequenzprotokoll und/oder die dazugehörigen Tabellen enthält/enthalten, nur in computerlesbarer Form, wie im Zusatzfeld betreffend das Sequenzprotokoll angegeben (siehe Abschnitt 802 der Verwaltungsvorschriften).</p>		
<p>4. Dieser Bericht enthält Angaben zu folgenden Punkten:</p> <p><input checked="" type="checkbox"/> Feld Nr. I Grundlage des Bescheids</p> <p><input type="checkbox"/> Feld Nr. II Priorität</p> <p><input type="checkbox"/> Feld Nr. III Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit</p> <p><input type="checkbox"/> Feld Nr. IV Mangelnde Einheitlichkeit der Erfindung</p> <p><input checked="" type="checkbox"/> Feld Nr. V Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung</p> <p><input type="checkbox"/> Feld Nr. VI Bestimmte angeführte Unterlagen</p> <p><input type="checkbox"/> Feld Nr. VII Bestimmte Mängel der internationalen Anmeldung</p> <p><input type="checkbox"/> Feld Nr. VIII Bestimmte Bemerkungen zur internationalen Anmeldung</p>		
Datum der Einreichung des Antrags  14.03.2005	Datum der Fertigstellung dieses Berichts  19.12.2005	
Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde   Europäisches Patentamt - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Bevollmächtigter Bediensteter  Bassanini, A  Tel. +31 70 340-2036	



**Feld Nr. I Grundlage des Berichts**

1. Hinsichtlich der **Sprache** beruht der Bericht auf der internationalen Anmeldung in der Sprache, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.
- ☐ Der Bericht beruht auf einer Übersetzung aus der Originalsprache in die folgende Sprache, bei der es sich um die Sprache der Übersetzung handelt, die für folgenden Zweck eingereicht worden ist:
- ☐ internationale Recherche (nach Regeln 12.3 und 23.1 b))
  - ☐ Veröffentlichung der internationalen Anmeldung (nach Regel 12.4)
  - ☐ internationale vorläufige Prüfung (nach Regeln 55.2 und/oder 55.3)
2. Hinsichtlich der **Bestandteile\*** der internationalen Anmeldung beruht der Bericht auf *(Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt)*:

**Beschreibung, Seiten**

1-14 in der ursprünglich eingereichten Fassung

**Ansprüche, Nr.**

1-19 in der nach Artikel 19 geänderten Fassung (ggf. mit einer Erklärung)

**Zeichnungen, Blätter**

1/3-3/3 in der ursprünglich eingereichten Fassung

☐ einem Sequenzprotokoll und/oder etwaigen dazugehörigen Tabellen - siehe Zusatzfeld betreffend das Sequenzprotokoll

3. ☐ Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung: Seite
- ☐ Ansprüche: Nr.
- ☐ Zeichnungen: Blatt/Abb.
- ☐ Sequenzprotokoll (*genaue Angaben*):
- ☐ etwaige zum Sequenzprotokoll gehörende Tabellen (*genaue Angaben*):

4. ☒ Dieser Bericht ist ohne Berücksichtigung (von einigen) der diesem Bericht beigelegten und nachstehend aufgelisteten Änderungen erstellt worden, da diese aus den im Zusatzfeld angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2 c)).

- ☐ Beschreibung: Seite
- ☒ Ansprüche: Nr. 1-19
- ☐ Zeichnungen: Blatt/Abb.
- ☐ Sequenzprotokoll (*genaue Angaben*):
- ☐ etwaige zum Sequenzprotokoll gehörende Tabellen (*genaue Angaben*):

\* Wenn Punkt 4 zutrifft, können einige oder alle dieser Blätter mit der Bemerkung "ersetzt" versehen werden.

# INTERNATIONALER VORLÄUFIGER BERICHT ÜBER DIE PATENTIERBARKEIT

Internationales Aktenzeichen  
PCT/EP2004/010545

---

**Feld Nr. V Begründete Feststellung nach Artikel 35 (2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung**

---

- |                                |                      |
|--------------------------------|----------------------|
| 1. Feststellung                |                      |
| Neuheit (N)                    | Ja: Ansprüche 1-19   |
|                                | Nein: Ansprüche      |
| Erfinderische Tätigkeit (IS)   | Ja: Ansprüche        |
|                                | Nein: Ansprüche 1-19 |
| Gewerbliche Anwendbarkeit (IA) | Ja: Ansprüche: 1-19  |
|                                | Nein: Ansprüche:     |

2. Unterlagen und Erklärungen (Regel 70.7):  
**siehe Beiblatt**

**Zu Punkt V**

**Begründete Feststellung hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung**

1. Es wird auf die folgenden Dokumente verwiesen:

- D1: US 2002/165830 A1 (KREMER GILLES) 7. November 2002 (2002-11-07)
- D2: WO 01/86539 A (HO TECK CHEONG ; CREDITEL S PTE LTD (SG); LIM KAY HIAN DANNY (SG)) 15. November 2001 (2001-11-15)
- D3: EP-A-1 065 634 (MIC SYSTEMS) 3. Januar 2001 (2001-01-03)
- D4: US 2001/037264 A1 (HUSEMANN DIRK ET AL) 1. November 2001 (2001-11-01)
- D5: US 2003/153298 A1 (EDER REINHARD ET AL) 14. August 2003 (2003-08-14)
- D6: US 2002/147658 A1 (KWAN KHAI HEE) 10. Oktober 2002 (2002-10-10)

2. **ÄNDERUNGEN (ARTIKEL 19 UND REGEL 70.2(c) PCT)**

- 2.1 Die Prüfungsabteilung ist der Meinung, daß die nach Artikel 19 geänderte Ansprüche 1-19 die Erfordernisse der Artikel 19(2) PCT nicht erfüllen. Die Gründe dafür sind die folgenden:
- 2.2 Der Ausdruck "für die Identifikationsnummer", der in der geänderten unabhängigen Ansprüchen 1 und 2 benutzt ist, setzt voraus, daß das vom Diensteanbieter geladete Konto unbedingt zur Identifikationsnummer verbunden ist und schließt z.B. den Fall aus, wonach die Identifikationsnummer vom Diensteanbieter nur benutzt wird, um die Identität des ersten Netzwerkteilnehmerknotens herauszufinden und die Transaktion mittels eines anderen, getrennten Kontos zu berechnen (vgl. z.B. D4, [0065]-[0066]).
- 2.3 Die ursprüngliche Fassung der Anmeldung verweist nur auf einem "beim zugehörigen Diensteanbieterknoten geführten Konto des ersten Netzwerkteilnehmerknotens" (vgl. die Beschreibung, Seite 5, Zeile 16-17 und Seite 10, Zeile 16-20; Anspruch 14). Die Möglichkeit, ein unbedingt zur Identifikationsnummer verbundenes Konto zu belasten wird in der ursprünglichen Fassung nur für bestimmte Ausführungsbeispiele (vgl. z.B.



Seite 3, Zeile 4-10 und 28-30; Seite 6, Zeile 31-35; Seite 12, Zeile 26-33) offenbart, während die Ansprüche breiter formuliert sind und breitgefächerte Ausführungsformen erfassen.

Der Gegenstand der geänderten Ansprüchen 1-19 geht daher über den Inhalt der Anmeldung in der ursprünglich eingereichten Fassung hinaus (Artikel 19 PCT).

- 2.4 Wegen der oben erwähnten Einwänden, wird die Prüfung auf die ursprünglich eingereichten Ansprüche beschränkt (Regel 70.2(c) PCT).

### 3. ERFINDERISCHE TÄTIGKEIT (ART. 33(3) PCT)

#### Unabhängige Ansprüche

- 3.1 Die vorliegende Anmeldung erfüllt nicht die Erfordernisse des Artikels 33(1) PCT, weil der Gegenstand des Anspruchs 1 nicht auf einer erfinderischen Tätigkeit im Sinne von Artikel 33(3) PCT beruht.
- 3.2 Der Gegenstand jenes Anspruchs definiert ein Verfahren zur Abwicklung einer elektronischen Transaktion, welches weitbekannte Methodenschritte zweier Klassen kombiniert. Es wird insbesondere Schritte aus bekannten Methoden zur Autorisierung einer elektronischen Transaktion mittels (mindestens) zwei verschiedener Kommunikationsnetzwerke mit Schritten aus bekannten Methoden zur Bezahlung solcher Transaktionen mittels bei Dienstprovider existierenden Kundenkonten kombiniert.
- 3.3 In der Methoden aus der ersten Klasse (vgl. z.B. Dokumente D1-D3) werden zwei Kommunikationsendgeräte, die mit zwei verschiedenen Kommunikationsnetzwerken verbunden sind, von einem Kunden benutzt. Wenn der Kunde mittels des ersten Geräts die Bezahlung initiiert, sendet ein Bezahlungsserver (o.ä.) einem Gerät eine Transaktionsnummer, die der Kunde mittels des anderen Geräts dem Bezahlungsserver zurücksendet. Bei Übereinstimmung dieser Transaktionsnummer mit derjenigen, die originell erzeugt worden war, wird die Transaktion bestätigt.

- 3.4 In der Methoden aus der zweiten Klasse (vgl. z.B. D4-D6) wird der Kunde in einer elektronischen Transaktion mittels seiner Identifikationsdaten in einem Kommunikationsnetzwerk (z. B. mittels seiner Mobilfunknummer) erkannt und belastet.
- 3.5 Der Gegenstand des Anspruchs 1 besteht aus einer Kombination weitbekannter Merkmalen von Methoden aus den beiden vorgegebenen Klassen, die keine erfinderische funktionelle Wechselwirkung ergibt. Diese Kombination besteht daher lediglich in einer Aneinanderreihung oder Nebeneinanderstellung bekannter Verfahren, die jeweils auf normale Art und Weise funktionieren, und kann nicht als erfinderisch betrachtet werden (Art. 33(3) PCT).

Der Gegenstand des Anspruchs 1 beruht daher nicht auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT).

- 3.6 Die gleiche Begründung gilt entsprechend für den unabhängigen Anspruch 2, worin eine Variante des Verfahrens vom Anspruch 1 definiert wird. Bei den Unterschieden zwischen diesen Ansprüchen handelt es sich nur um naheliegenden Verfahrensschritte, aus denen der Fachmann ohne erfinderisches Zutun den Umständen entsprechend auswählen würde, um die elektronische Transaktion abzuwickeln.

Der Gegenstand des Anspruchs 2 beruht daher nicht auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT).

#### Abhängige Ansprüche

- 3.7 Die abhängigen Ansprüche 3-19 enthalten keine Merkmale, die in Kombination mit den Merkmalen irgendeines Anspruchs, auf den sie sich beziehen, die Erfordernisse des PCT in bezug auf erfinderische Tätigkeit erfüllen. Die zusätzlichen Merkmale, die darin definiert werden, sind aus dem Stand der Technik allgemein bekannt und liegen im Rahmen dessen, was ein Fachmann aufgrund der ihm geläufigen Überlegungen zu tun pflegt, zumal die damit erreichten Vorteile ohne weiteres im Voraus zu übersehen sind (vgl. z.B. D1-D6 und die entsprechenden im Recherchenbericht angegebenen Textstellen).

Der Gegenstand der Ansprüche 3-19 beruht daher nicht auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT).



(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
15 November 2001 (15.11.2001)

PCT

(10) International Publication Number  
**WO 01/86539 A1**

(51) International Patent Classification<sup>7</sup>: **G06F 17/60**

(21) International Application Number: **PCT/SG00/00180**

(22) International Filing Date:  
3 November 2000 (03.11.2000)

(25) Filing Language: **English**

(26) Publication Language: **English**

(30) Priority Data:  
09/570,207 12 May 2000 (12.05.2000) **US**

(71) Applicant (for all designated States except US): **CRED-ITEL (S) PTE LTD** [SG/SG]; 20 Maxwell Road #04-02, Maxwell House, Singapore 069113 (SG).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **LIM, Kay, Hian,**

**Danny** [SG/SG]; 48 Watten Estate Road, Singapore 287636 (SG). **HO, Teck, Cheong** [SG/SG]; 77 Nim Road #10-02, Singapore 807586 (SG).

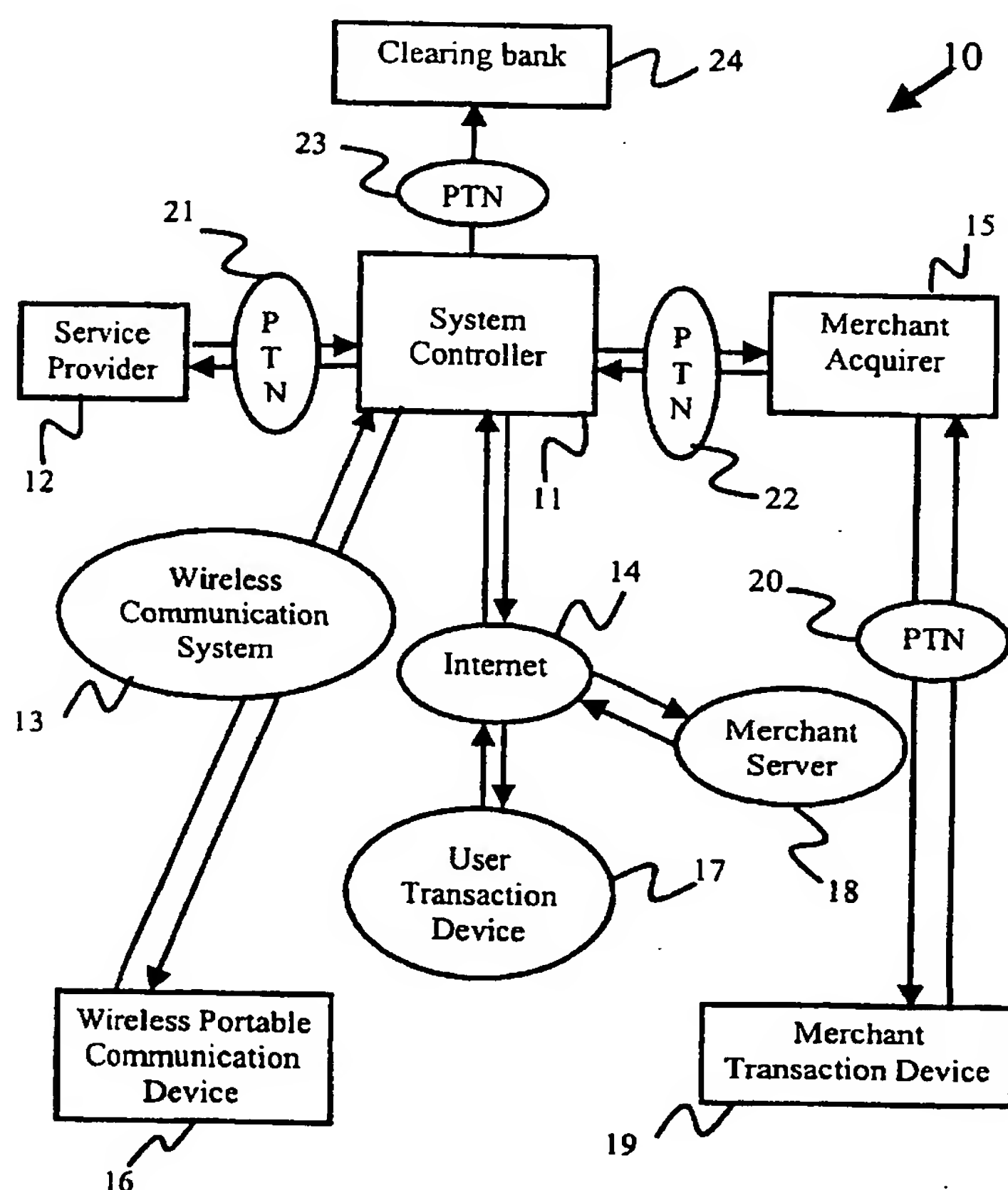
(74) Agent: **ELLA CHEONG MIRANDAH & SPRUSONS PTE LTD**; Robinson Road Post Office, P.O. Box 1531, Singapore 903031 (SG).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: **ELECTRONIC TRANSACTION SYSTEM AND METHODS THEREOF**



(57) Abstract: An electronic transaction system (10) for validating electronic transactions of a user of system (10) is described. System (10) includes a system controller (11) that couples to a service provider (12) of a wireless communication system (13), the Internet (14) and a merchant acquirer (15). System (10) supports electronic transactions such as payment for goods and services. An electronic transaction is initiated from either a user transaction device (17) or a merchant transaction device (19). Controller (11) then communicates transaction and user information with devices (17, 19) via the Internet (14) or a private transaction network (20). In one type of transaction, the user information has an identification code identifying communication device (16). In another type of transaction, a transaction code is sent to communication device (16). Upon controller (11) verifying the user, the transaction is validated and a message is sent directly to communication device (16).

WO 01/86539 A1

WO 01/86539 A1



IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

**Published:**

— *with international search report*

## **ELECTRONIC TRANSACTION SYSTEM AND METHODS THEREOF**

### **Field of the Invention**

5           This invention relates to non-cash electronic transactions such as credit card payments for goods and services. In particular, this invention relates to an electronic transaction system to prevent or at least alleviate transaction fraud and methods thereof.

### **Background**

10           Payments for goods and services are made through various commercial instruments such as, for example, cash, checks, and credit cards. Use of non-cash instruments has grown both in terms of volume as well as popularity. This use is expected to accelerate especially with the proliferation of electronic commerce (e-  
15 commerce) via the Internet.

          For non-cash instruments and, in particular, credit cards, the accuracy of identifying and authenticating purchasers is critical in order to avoid payment fraud. To identify or authenticate a user of a credit card, a merchant has to examine the  
20 credit card to detect forgery as well as verify data stored in a magnetic data strip of the credit card. Typically, such data includes user information that is electronically extracted and processed to validate an electronic transaction. Processing generally involves electronically relaying the user information to a company that issued the credit card or agents of such a company.

25           Generally, fraudulent use of credit cards in face-to-face transactions involves criminal syndicates because the entire process for such fraudulent use requires multiple parties and large resources to produce forged credit cards. While credit card companies use more sophisticated printing processes to prevent unauthorized  
30 reproduction of credit cards, such processes are still accessible to criminal syndicates.

In addition to the physical appearance of a credit card, the data stored in the magnetic data strip can be copied or reproduced. For electronic transactions such as purchasing goods via the Internet, fraud is more easily committed because such fraud  
5 only requires the data stored for a credit card. This is because the credit card does not need to be physically provided to validate Internet transactions. Hence, individuals who have access to the data of the credit cards can commit credit card fraud via Internet transactions.

10 The above problems of fraud in an electronic transaction system are further compounded by the possibility of unauthorized access to locations in which credit card information of customers are stored. Security of these locations is not practically monitored by any public or private regulatory bodies and, currently, does not conform to any internationally acceptable security standards.

15 Conventionally, an electronic transaction system has locations at which confidential information is stored. The electronic transaction system typically enables user access via assigned user identification (ID) and passwords. Generally, to protect against unauthorized access to such locations, user accounts are suspended  
20 after a predetermined number of attempts . However, suspending user accounts is inconvenient to users as well as service providers because computer hackers can then cause widespread access denial. Such widespread access denial requires considerable efforts to reinstate suspended user accounts. Reinstating suspended user accounts can be costly in terms of time, loss of use, administrative expenses and, most  
25 importantly, loss of confidence in an electronic transaction system.

Consequently, verification and authentication have to be reduced to a practical level to accommodate users having varying levels of technological knowledge and capability. On the other hand, the protection of confidential  
30 information such as user ID and passwords has to be maintained at a sufficient level of security to attain user confidence.

Credit card fraud accounts for significant losses of credit card companies and merchants that provide for credit card billings. Without major enhancements to existing credit card payment systems, the impact of credit card fraud, especially for merchants who conduct business on the Internet, is likely to increase. Therefore, in view of the above problems and constraints, there is a need for an electronic transaction system to prevent or at least alleviate credit card fraud and yet that has security features that are practically applied by users.

## 10 Summary

In accordance with one aspect of the invention, there is disclosed an electronic transaction system for validating a transaction of a user of the electronic transaction system, the electronic transaction system having a system controller, includes:

15 means for receiving, by the system controller of the electronic transaction system, transaction information and user information from a transaction device coupled to the system controller, the transaction information and the user information being respectively associated with the transaction and the user;

20 means for receiving, by the system controller from a wireless portable communication device associated with the user, at least one identification code associated with the wireless portable communication device;

25 means for verifying, by the a system controller, the at least one identification code and the user information based upon registered information of the user, the registered information being stored in association with the system controller;

30 and

means for determining, by the controller, whether to validate the transaction in response to the verifying.

Generally, the electronic transaction system can further include means for  
5 invalidating the transaction when either the at least one identification code or the user information is not verified.

Typically, the determining means can include means for checking credit information of the user, the credit information being stored in association with the  
10 system controller.

More typically, the electronic transaction system can further include means for validating the transaction based upon the checking.

15 Yet more typically, the electronic transaction system can further include means for transmitting at least one message to the wireless portable communication device upon validating the transaction.

Generally, the means for receiving the transaction information and the user  
20 information can include means for prompting the user to provide at least one input to obtain at least some of the user information.

In accordance with another aspect of the invention, there is disclosed an \_\_\_\_\_  
electronic transaction system for validating a transaction of a user of the electronic  
25 transaction system, the electronic transaction system having a system controller, includes:

means for receiving, by the system controller of the electronic transaction system, transaction information and user information from a transaction device coupled to the system controller, the transaction information and the  
30 user information being respectively associated with the transaction and the user;



means for transmitting, by the system controller to a wireless portable communication device associated with the user, at least one transaction code associated with the transaction;

5

means for receiving, by the system controller via the transaction device, the at least one transaction code for verification;

and

10

means for determining, by the system controller, whether to validate the transaction based upon the verification.

Generally, the electronic transaction system can further include means for  
15 invalidating the transaction when the verification of the at least one transaction code fails.

Typically, the determining means can include means for checking credit  
information of the user, the credit information being stored in association with the  
20 system controller.

More typically, the electronic transaction system can further include means  
for validating the transaction based upon the checking.

25 Yet more typically, the electronic transaction system can further include  
means for transmitting at least one message to the wireless portable communication  
device upon validating the transaction.

Generally, the means for receiving the transaction information and the user  
30 information can include means for prompting the user to provide at least one input to  
obtain at least some of the user information.

In accordance with another aspect of the invention, there is disclosed a method for validating a transaction of a user of an electronic transaction system, the method including the steps of:

5           receiving, by a system controller of the electronic transaction system, transaction information and user information from a transaction device coupled to the system controller, the transaction information and the user information being respectively associated with the transaction and the user;

10           receiving, by the system controller from a wireless portable communication device associated with the user, at least one identification code associated with the wireless portable communication device;

15           verifying, by the a system controller, the at least one identification code and the user information based upon registered information of the user, the registered information being stored in association with the system controller;

and

20           determining, by the system controller, whether to validate the transaction based upon the verifying step.

Generally, the method can further include the step of invalidating the transaction when either the at least one identification code or the user information is  
25   not verified.

Typically, the determining step can include the step of checking credit information of the user, the credit information being stored in association with the system controller.

30

More typically, the method can further include the step of validating the transaction based upon the checking step.

Yet more typically, the method can further include the step of transmitting at  
5 least one message to the wireless portable communication device upon validating the transaction.

Generally, the step of receiving the transaction information and the user  
information can include the step of prompting the user to provide at least one input to  
10 obtain at least some of the user information.

In accordance with another aspect of the invention, there is disclosed a method for validating a transaction of a user of an electronic transaction system, the method including the steps of:

15 receiving, by a system controller of the electronic transaction system, transaction information and user information from a transaction device coupled to the system controller, the transaction information and the user information being respectively associated with the transaction and the user;

20 transmitting, by the system controller to a wireless portable communication device associated with the user, at least one transaction code associated with the transaction;

25 receiving, by the system controller via the transaction device, the at least one transaction code for verification;

and

30 determining, by the system controller, whether to validate the transaction based upon the verification.

Generally, the method can further include the step of invalidating the transaction when the verification of the at least one transaction code fails.

Typically, the determining step can include the step of checking credit  
5 information of the user, the credit information being stored in association with the system controller.

More typically, the method can further include the step of validating the transaction based upon the checking step.

10

Yet more typically, the method can further include the step of transmitting at least one message to the wireless portable communication device upon validating the transaction.

15 Generally, the step of receiving the transaction information and the user information can include the step of prompting the user to provide at least one input to obtain at least some of the user information.

20 In accordance with another aspect of the invention, there is disclosed a computer program product with a computer usable medium having a computer readable program code means embodied therein for validating a transaction of a user of an electronic transaction system having a system controller, the computer program product including:

25 computer readable program code means for receiving, by the system controller of the electronic transaction system, transaction information and user information from a transaction device coupled to the system controller, the transaction information and the user information being respectively associated with the transaction and the user;

30

computer readable program code means for receiving, by the system controller from a wireless portable communication device associated with the user, at least one identification code associated with the wireless portable communication device;

5

computer readable program code means for verifying, by the system controller, the at least one identification code and the user information based upon registered information of the user, the registered information being stored in association with the system controller;

10

and

computer readable program code means for determining, by the controller, whether to validate the transaction in response to the verifying.

15

Generally, the computer program product can further include computer readable program code means for invalidating the transaction when either the at least one identification code or the user information is not verified.

20

Typically, the computer readable program code means for determining can include computer readable program code means for checking credit information of the user, the credit information being stored in association with the system controller.

25

More typically, the computer program product can further include computer readable program code means for validating the transaction based upon the checking.

Yet more typically, the computer program product can further include computer readable program code means for transmitting at least one message to the wireless portable communication device upon validating the transaction.

30

Generally, the computer readable program code means for receiving the transaction information and the user information can include computer readable program code means for prompting the user to provide at least one input to obtain at least some of the user information.

5

In accordance with another aspect of the invention, there is disclosed a computer program product with a computer usable medium having a computer readable program code means embodied therein for validating a transaction of a user of an electronic transaction system having a system controller, the computer program product including:

10

computer readable program code means for receiving, by the system controller of the electronic transaction system, transaction information and user information from a transaction device coupled to the system controller, the transaction information and the user information being respectively associated with the transaction and the user;

15

computer readable program code means for transmitting, by the system controller to a wireless portable communication device associated with the user, at least one transaction code associated with the transaction;

20

computer readable program code means for receiving, by the system controller via the transaction device, the at least one transaction code for verification;

25

and

computer readable program code means for determining, by the controller, whether to validate the transaction based upon the verification.



Generally, the computer program product can further include computer readable program code means for invalidating the transaction when the verification of the at least one transaction code fails.

5 Typically, the computer readable program code means for determining includes computer readable program code means for checking credit information of the user, the credit information being stored in association with the system controller.

10 More typically, the computer program product can further include computer readable program code means for validating the transaction based upon the checking.

Yet more typically, the computer program product can further include computer readable program code means for transmitting at least one message to the wireless portable communication device upon validating the transaction.

15 Generally, the computer readable program code means for receiving the transaction information and the user information can include computer readable program code means for prompting the user to provide at least one input to obtain at least some of the user information.

20

### **Brief Description of the Drawings**

Embodiments of the invention are described hereinafter with reference to the drawings, in which:

25 FIG. 1 is a schematic block diagram illustrating an electronic transaction system in accordance with a preferred embodiment of the invention;

FIG. 2 is a flowchart illustrating processing of an identification code of a wireless portable communication device in the electronic transaction system of FIG. 1;

30

1;

FIG. 3 is a flowchart illustrating a user registration process to register users of for the electronic transaction system of FIG. 1;

FIG. 4 is a flowchart illustrating a process for a user of the electronic transaction system of FIG. 1 to change a user ID and/or password;

FIG. 5 is a schematic block diagram of a system controller of the electronic transaction system of FIG. 1;

FIGs. 6a to 6c are flowcharts illustrating a method for processing a typical Internet transaction of the electronic transaction system of FIG. 1;

FIGs. 7a to 7c are flowcharts illustrating a method for processing a typical face-to-face transaction of the electronic transaction system of FIG. 1; and

FIG. 8 is a block diagram of an example of a computer system capable of processing electronic transactions in the electronic transaction system of FIG. 1.

### Detailed Description

An electronic transaction system, a method and a computer program product for validating electronic transactions of users of the electronic transaction system in accordance with a preferred embodiment of the invention are described. In the following, numerous details are provided for a more thorough description. It shall be apparent to one skilled in the art, however, that the invention may be practised without such details. In other instances, well-known details have not been described at length so as not to obscure the invention.

The advantages of the preferred embodiment of the invention are manifold. One advantage is that electronic transactions, such as, for example, payments or change of user information are effected using different communication media. This enhances security of the electronic transaction system. Thus, opposite parties of, for

example, a payment transaction can verify information relating to each other and to the payment transaction with the different communication media before validating the payment transaction.

5 Another advantage of the preferred embodiment of the invention is that security and usability of the preferred embodiment of the invention can be easily established with existing wireless communication systems such as mobile phone networks. This makes for an easier acceptance of the preferred embodiment of the invention as users need not have to learn completely new processes.

10

Yet a further advantage of the preferred embodiment of the invention is that infrastructure support for implementing the preferred embodiment is at least partly available when used with existing mobile phone networks having mobile phones with roaming capabilities.

15

Referring now to FIG. 1, a schematic block diagram of an electronic transaction system 10 in accordance with a preferred embodiment of the invention is illustrated. The electronic transaction system 10 supports transactions such as, for example, change of user information or payment for goods and services. The  
20 electronic transaction system 10 includes a system controller 11. The system controller 11 couples to a service provider 12, a wireless communication system 13, the Internet 14 and a merchant acquirer 15.

The merchant acquirer 15 is responsible for recruitment of merchants  
25 participating in the electronic transaction system 10. Merchants are sellers of goods and services who have joined the electronic transaction system 10 and accept payment through the electronic transaction system 10 either for face-to-face and/or Internet transactions. For face-to-face transactions, the merchant acquirer 15 arranges to install, maintain and route all transactions originating from a merchant location.  
30 The merchant acquirer 15 thus coordinates with merchants in promoting use of the electronic transaction system 10. In addition, the merchant acquirer 15 is a settlement

agent for participating merchants and is responsible for the proper conduct of such participating merchants in accordance to rules and regulations of the electronic transaction system 10.

5           The wireless communication system 13 supports at least one wireless portable communication device 16. The wireless communication system 13 can be, for example, a mobile phone network. In such a mobile phone network, the wireless portable communication device 15 is a mobile phone for a user to communicate with the system controller 11.

10

As for transactions via the Internet 14, a user can access the system controller 11 using a transaction device 17. The transaction device 17 can be, for example, a computer system coupled to the Internet 14. Typically, the user browses a merchant website associated with the merchant server 18 using the computer system prior to making a transaction. The transaction can be, for example, a purchase of goods or services provided via the merchant website.

When a user makes transactions at a merchant location, a merchant transaction device 19 is used to access the system controller 11. The merchant transaction device 19 couples to the merchant acquirer via a private transaction network 20.

Connection between the system controller 11 to the merchant acquirer 15 and to the service provider 12 is via private transaction networks (PTNs) 20,21,22, respectively. The use of the PTNs 20,21,22 enables control of communications between the system controller 11 and the service provider 12 or the merchant acquirer 15. Such control can be applied to leased lines, dial-up lines or wireless data communication networks used in the PTNs 20,21,22. Furthermore, the communications can be further protected by cryptography methods to encrypt data in such communications. Thus, controlling communications using the PTNs 20,21,22 can prevent or at least alleviate unauthorized access to the communications.

It is to be noted that transaction devices 17,19 include user input devices that are not shown in FIG. 1. Such user input devices enable a user to provide information related to a transaction that is being transacted.

5

The system controller 11 also couples via a PTN 23 to at least one clearing bank 24 that is collectively indicated by a single block. The at least one clearing bank 24 supports financial transactions of the electronic transaction system 10 and is responsible for settlement of user accounts of users from the service provider 12 or the merchant acquirer 15.

In using the electronic transaction system 10, use of the wireless portable communication device 16 is required at some stage of a transaction. In one embodiment of the invention, an identification code that is unique to the wireless portable communication device 16 is required for some transactions. Such an identification code is possible for mobile phones. This is because mobile telephone manufacturers as well as mobile telephone service providers are continually improving or at least maintaining security features of mobile telephony. Consistent with this development, most users or subscribers are currently registered with a unique identification code. Such an identification code enables a mobile telephone to operate when in the coverage area of different mobile telephone service providers. The identification code may include alphanumeric characters.

Referring now to FIG. 2, a flowchart illustrates processing 30 of an identification code received by the system controller 11. The identification code is communicated to the system controller 11 when a system feature is selected. At step 31, a user communicates the identification code to the electronic transaction system 10 using the wireless portable communication device 16 via, for example, one or more of the following communication modes:

- 30           a) Interactive voice response (IVR);  
            b) Short message system (SMS); and



c) Wireless application protocol (WAP).

These communication modes cater to users who have varying levels of comfort in adapting to complex technology.

5           Use of the identification code enables the system controller 11 to ascertain the intended purpose of the user in selecting the system feature at step 32. This intended purpose can be to enable a system feature such as, for example, changing user information or making a purchase of goods or services. In providing the identification code together with selecting a system feature, the system controller 11  
10       can then enable a selected system feature to be subsequently processed. The user information can include a user identification (ID) or password. It is assumed that only a registered user of the wireless portable communication device 16 can invoke the identification code for a transaction. Unauthorized use of the wireless portable communication device 16 is not likely unless an unauthorized user knows the user ID  
15       or password. The system controller 11 then time logs the identification code at decision step 33. Within a specified time limit that is configurable as a predetermined transaction parameter, the selected system feature is enabled at step 34 with a "No" from decision step 33. The user can then proceed with the selected system feature. After the specified time limit expires and if the user does not complete the intended  
20       purpose, the system controller 11 times out the identification code. Thereafter, the system controller 11 generates an output message at step 35 to inform the user via the wireless portable communication device 16 using, for example, SMS.

          In providing for process 30, the electronic transaction system 10 has an  
25       additional security procedure in which the user is clearly identified. This is because the identification code can only originate from the wireless portable communication device 16 that is registered to the user. Furthermore, with the identification code, the electronic transaction system 10 is protected from computer hacking or other forms of malicious intentions. This is because access to the system controller 11 requires  
30       completion of the process 30 before any subsequent processing or access can continue.



The identification code serves two purposes. First, it verifies that the user has an intention to perform a function such as changing an assigned user ID and/or password, or making a purchase. Second, the identification code is an additional security feature that prevents unauthorized attempts to query a database for a correct match of the user ID and password. Hence, use of the identification code, in conjunction with a user ID and password, provides the electronic transaction system 10 with a security feature that is practical and easy to use.

Also, use of the system controller 11 ensures confidential information pertaining to transactions or users are not transmitted and/or stored on any other servers. Such users need to register with the system controller 11 in order to use the electronic transaction system 10.

Referring now to FIG. 3, a user registration process 40 to register users for the electronic transaction system 10 is illustrated. In collaboration with the service provider 12 of FIG. 1, subscribers of the wireless communication system 13 are identified from databases of the service provider 12. These databases are represented using a single block 41 in FIG. 3. The service provider 12 facilitates recruitment of users from the subscribers and is also a collection agent for purchases incurred by these users. The service provider 12 is also responsible for real time updating of user data with the system controller 11.

The subscribers are invited to join as users of the electronic transaction system 10 at step 42. Each subscriber is provided with an application form and pre-assigned with a user ID and a password. The user ID is unique in that no two users are given the same user ID. Thereafter, the subscriber has a choice of whether or not to register as a user at decision step 43. If the subscriber declines or ignores an invitation resulting in a 'No' from decision step 43, the user registration process 40 for that subscriber terminates at step 44. Otherwise, a 'Yes' from decision step 43 is

obtained when a subscriber submits the application form to the service provider 12 at step 45.

To complete the user registration process 40 for a subscriber, staff of the service provider 12 inputs user information pertaining to that subscriber at step 46. Thereafter, the user information is provided, via the private transaction network (PTN) 21, for storage into at least one storage location of the electronic transaction system 10 at step 47. This at least one storage location is associated with the system controller 11.

10

Following completion of the user registration process 40, a user account is activated. A request by the user to enable a system feature such as to change the user ID or password is processed by the system controller 11 using a process 50 illustrated by the flowchart of FIG. 4. The user can be connected to the system controller 11 via, for example, the Internet 14.

15

Process 50 starts when the system controller 11 requests an identification code from the user at step 51. The user identification code is provided using the process 30. Upon selecting a system feature and, consequently providing the identification code, the user inputs a user ID at step 52. Thereafter, the system controller 11 determines whether the user ID and the identification code are correctly matched or verified at decision step 53. With a 'No' from decision step 53, the system controller 11 determines at decision step 54 whether less than three attempts have been made by the user to enter the user ID or whether a timeout has occurred. The system controller 11 has a timeout feature that is activated if the user ID is not received within a predetermined time period. With a 'No' following decision step 54, the process 50 returns to step 52 in which the system controller 11 awaits the user to re-enter the user ID and password. Otherwise, with a 'Yes' following decision step 54, the process 50 proceeds to step 55. At step 55, the system controller 11 terminates the process 50.

20

25

30

With a 'Yes' from decision step 53, the process 50 continues to step 56 in which the system controller 11 prompts for a password. Thereafter, the system controller 11 determines at decision step 57 whether the password is verified at decision step 57. For a 'No' following decision step 57, the system controller 11  
5 determines at decision step 58 whether less than three attempts have been made by the user to enter the password or whether the timeout has occurred. With a 'Yes' following decision step 58, the process 50 proceeds to step 59. At step 59, the system controller 11 terminates the process 50, notifies the service provide 12 about the failed attempts to access the system controller 11 and suspends the user account.

10

Following a 'Yes' from decision step 57, the process 50 continues to step 60 at which the user inputs a new user ID. The new user ID has to conform with predetermined parameters in order to meet security requirements of the electronic transaction system 10. At decision step 61, the system controller 11 checks for  
15 uniqueness of the new user ID. If the new user ID is not unique, the process 50 returns with a 'No' to step 60. Otherwise, once the new user ID is determined to be unique, the process 50 proceeds with a 'Yes' to step 62.

At step 62, the user inputs a new password and the process 50 continues with  
20 step 63 at which the user has to re-enter the new password for confirmation. With the new password ascertained, the system controller 11 verifies at decision step 64 whether the new password conforms to security requirements of the electronic transaction system 10. A 'No' from decision step 64 results in the process 50 returning to step 63 to input another new password. Otherwise, a 'Yes' following  
25 decision step 64 ends the process 50 at step 65 in which the user is informed of the change in the user ID and/or password via an SMS transmitted to the wireless portable communication device 16.

Thus far, user account set-up or changes to a user account initiated by a user  
30 of the electronic transaction system 10 has been described. The set-up and changes involve only the user accessing the system controller 11 via the wireless

communication system 13 or the Internet 14. Reference shall now be made to FIG. 5 to describe features of the system controller 11.

Referring now to FIG. 5, a schematic block diagram of the system controller 11 is illustrated. The system controller 11 maintains all user information and transaction records. The service provider 12 can update the user information on-line. The system controller 11 serves as an authenticating body for all transactions of the electronic transaction system 10, manages usability of the electronic transaction system 10 via the Internet 14, enables transaction confirmations to merchants and provides settlement services to service providers and merchant acquirers participating in the electronic transaction system 10.

The system controller 11 supports two verification processes as described hereinbefore. Specifically, one of the two verification processes is to verify the identification code associated with the wireless portable communication device 16 or the merchant acquirer 15. The other one of the two verification processes is to verify the user ID and password of a user. These two verification processes are separately processed to isolate the user information and enhance security of the user information and the system controller 11.

20

For non-Internet transactions, the system controller 11 has a communications controller 71, a user account server 72 and a database server 73. The communications controller 71 controls communications between the electronic transaction system 10 and either the wireless portable communication device 16 or the merchant acquirer. The user account server 72 couples to the communications controller 71 and the database server 73 to support transactions in which transaction information or user information, such as user IDs and/or passwords, is to be verified. The database server 73 accesses information stored in a storage device 74 of the system controller 11.

30

For Internet transactions, the system controller 11 has a firewall 75, a Web server 76, an applications server 77 and a database server 78. The firewall 75

provides a security shield for access to the system controller 11. The Web server 76 and the applications server 77 supports users who access the system controller 11 via the Internet 14. The database server 78 accesses information stored in the storage device 74 of the system controller 11. It is to be noted that the storage device 74 is  
5 common for the two verification processes.

Transactions in the electronic transaction system 10 can be carried out either through the Internet via the user transaction device 17 or face-to-face at a merchant location via the merchant transaction device 19. Typically, these transactions require  
10 the following procedures for completion:

- a) offer of goods and/or services by a merchant;
- b) acceptance of the offer;
- c) payment for the goods and/or services; and
- d) delivery and receipt of the goods and/or services.

15

Typical transactions for the electronic transaction system 10 are described with reference to the system controller 11 using FIGs. 6a to 6c and FIGs. 7a to 7c.

Referring now to FIGs. 6a to 6c, a method 100 for a typical Internet  
20 transaction of the electronic transaction system 10 is illustrated with a flowchart. Starting at step 101, a user is logged onto the Internet 14 to browse a merchant Website supported by the merchant server 18. Prices and description of goods and services are displayed to the user via the user transaction device 17. After selecting one or more items to purchase, the user is typically queried as to a preferred mode of  
25 payment for the items. This payment query is represented by decision box 102 in which a controller of the merchant transaction device 19 determines whether the payment mode selected requires use of the electronic transaction system 10. Generally, merchant Websites offer different modes of payment for Internet transactions. If the user selects other payment modes, then the method 100 continues  
30 with a 'No' to step 103. Otherwise, if the user selects the payment mode of the electronic transaction system 10, then the method 100 continues with step 104 in



which the controller of the merchant transaction device 19 establishes a connection between the user transaction device 17 and the system controller 11. In addition, at step 104, a computer program script is sent to the user transaction device 17 to initiate communications with the system controller 11. Communications between the user transaction device 17 and the system controller 11 is encrypted using known encryption techniques such as, for example, SSL™ (Secure Sockets Layer).

The method 100 continues to step 105 in which the system controller 11 requests the user to issue an identification code associated with the wireless portable communication device 16. This requires the user to provide the identification code as described in the process 30. In addition, the system controller 11 extracts transaction information of the purchase from the merchant transaction device 19. Following step 105, the method 100 continues to step 106 of FIG. 6b in which the user inputs a user ID. This user ID is then verified, at decision step 107, with the identification upon reception of the latter by the system controller 11. It is to be noted that unless the system controller 11 receives the identification code associated with the wireless portable communication device 16 of the user, the method 100 cannot continue. Hence, the system controller 11 has a timeout feature that is activated if the password is not received within a predetermined time period. Thus, the system controller 11 also monitors the predetermined time period at decision step 107. With a 'No' following decision step 107, the method 100 continues to decision step 108. At decision step 108, the system controller keeps count of the number of failed attempts at verifying the user ID with the identification code and also determines whether the predetermined time period has expired. For less than three failed attempts, the system controller 11 returns the method 100 with a 'No' back to step 106. Otherwise, when three failed attempts have been recorded or the predetermined time period has expired, the method 100 proceeds with a 'Yes' to step 109. At step 109, the system controller 11 terminates the method 100 for this transaction.

Following a 'Yes' from decision step 107, the method 100 continues to step 111 in which the system controller 11 prompts the user to provide a password.



Thereafter, the method 100 continues to decision step 112 in which the system controller 11 determines whether the password has been received and verified. In decision step 112, the timeout feature is again activated if the password is not received within the predetermined time period. Hence, for a 'No' in decision step 5 112, the method 100 continues to decision step 113 in which the system controller keeps count of the number of failed attempts and monitors the predetermined time period.

For a 'Yes' following decision step 113, the method 100 continues to step 10 114 in which the system controller 11 terminates the transaction. In addition, at step 114, the system controller 11 also notifies the service provider 12 of the failed attempts to complete the transaction and suspends the user account. Otherwise, the method 100 returns to step 111 to await another password input from the user following a 'No' from decision step 113.

15  
Returning to decision step 112, the method 100 continues to step 115 in FIG. 6c in which the system controller 11 checks credit information of the user. In particular, the credit limit of the user is determined at decision step 116 in order to continue the method 100. When the transaction is not within the credit limit of the 20 user, the method 100 proceeds with a 'No' to step 117. At step 117, the system controller 11 terminates the transaction and sends a message to the user via the wireless portable communication device 16 to request that the user checks with the service provider 12 on the credit limit. In addition, at step 117, the system controller 11 informs the service provider 12 on the incomplete transaction because of 25 insufficient credit limit.

The method 100 continues with a 'Yes' from decision step 116 to step 118 at which the system controller 11 informs the user that the transaction is approved. Thereafter, at step 119, the system controller 11 sends to the wireless portable 30 communication device 16 an SMS to confirm the transaction. With the transaction confirmed, the system controller 11 updates a transaction log at step 120 and updates

the merchant server 18 with an approval code for the transaction at step 121. The method 100 then terminates at step 121.

Referring now to FIGs. 7a to 7c, a method 200 for a typical face-to-face transaction of the electronic transaction system 10 is illustrated with a flowchart. For the method 200, the user is at a merchant location. The merchant location has the merchant transaction device 19 for the user to access the electronic transaction system 10. Hence, upon the user deciding to make a transaction such as payment for a purchase, the merchant transaction device 19 is activated to connect to the system controller 11 via the merchant acquirer 15. Connection between the merchant transaction device 19 and the merchant acquirer 15 uses the PTN 20 to ensure security of transactions therebetween.

Starting at step 201 in FIG. 6a, the merchant transaction device 19 establishes a connection to the system controller 11. Thereafter, transaction information for the transaction is provided to the system controller 11 at step 202. Upon receiving the transaction information, the system controller 11 then generates a request for the user ID and the password at step 203.

In response to the request, the user then inputs the user ID and the password at the merchant transaction device 19 at step 204 in FIG. 6b. The user ID and the password is then transmitted back to the system controller 11 from the merchant transaction device 19. Receiving the user ID and the password, the system controller 11 then determines at decision step 205 whether the user ID and the password matches user information stored at the system controller 11. The system controller 11 in decision step 205 also applies the timeout feature. With a 'No' from decision step 205, the method 200 continues to decision step 206 in which the system controller 11 determines whether there have been three failed attempts to verify the user ID and the password for the user. For a 'Yes' following decision step 206, the system controller 11 terminates the transaction at step 207. Otherwise, for a 'No' following decision step 206, the method 200 returns to step 204.

Returning back to decision step 205, the method 200 continues with a 'Yes' to step 208 at which the system controller 11 sends a transaction code to the user via the wireless portable communication device 16. The system controller 11 randomly  
5 generates the transaction code. Upon receiving the transaction code in, for example, an SMS, the user then inputs the transaction code at the merchant transaction device 19 at step 209. Thereafter, the system controller 11 verifies the transaction code to determine validity of the user at decision step 210.

10 With a 'No' following decision step 210, the process 200 continues to decision step 211. At decision step 211, the system controller 11 determines if three failed attempts has occurred or if the predetermined time period has expired. With a 'Yes' from decision step 211, the system controller 11 terminates the transaction at step 212. At step 212, the system controller 11 also notifies the service provider 12 of  
15 the terminated transaction and suspends the user account of the user.

Returning to decision step 210, and upon verification of the transaction code with a 'Yes', the method 200 continues to step 213 in FIG. 7c. At step 213, the system controller 11 checks credit information of the user to determine, for example,  
20 the user's credit limit. Thereafter, at decision step 214, if the credit limit is exceeded, a 'No' is generated and the method 200 continues to step 215. At step 215, the system controller 11 terminates the transaction and sends a message to the user via the wireless portable communication device 16 to request that the user checks with the service provider 12 on the credit limit. In addition, at step 215, the system  
25 controller 11 informs the service provider 12 on the incomplete transaction because of insufficient credit limit.

The method 200 continues with a 'Yes' from decision step 214 to step 216 at which the system controller 11 informs the user that the transaction is approved.  
30 Thereafter, at step 217, the system controller 11 sends the wireless portable communication device 16 an SMS to confirm the transaction. With the transaction

confirmed, the system controller 11 updates a transaction log at step 218 and updates the merchant server 18 with an approval code for the transaction at step 219. The method 100 then terminates at step 219.

5 For decision steps 116 and 214 in the methods 100 and 200, respectively, the credit limit of the user for a purchase is determined based on a rule table defined by the service provider 12. For example, the rule table can define the following:

- a) Maximum single purchase;
- b) Domicile of a merchant using an exclusion table;
- 10 c) Currency of purchase using an exclusion table for foreign exchange controls;
- d) Purchase limit for shipment to address other than the user's.

It is to be noted that the electronic transaction system 10 cannot assist users in  
15 evaluating a merchant from with whom they intend to make a purchase. However, merchants who are guilty of any unscrupulous dealings shall not be allowed to continue participating in the electronic transaction system 10.

It is further to be noted that the method 200 can be applied for Internet  
20 transactions. In other words, the electronic transaction system 10 can be configured such that a user of the user transaction device 17 is required to provide a transaction code to the system controller 11 using the wireless portable communication device 16. This depends on how much security is desired by users of the electronic transaction system 10.

25

To protect honest and reliable merchants, the electronic transaction system 10 ensures that a user is properly identified and has sufficient credit limit to complete a transaction. Thus, the electronic transaction system 10 facilitates the two transactions describe in the methods 100 and 200.

30

The transaction log mentioned in step 120 of the method 100 and step 216 in the method 200 keeps track of all failed attempts to log onto a user account.

5 The electronic transaction system 10 as described above provides for global usage as users are not restricted to a physical location when using the wireless portable communication device 16. Furthermore, infrastructure support for the electronic transaction system 10 is at least partly available if the wireless communication system 13 is implemented with existing mobile phone networks having mobile phones with roaming capabilities.

10 The system controller 11 in the preferred embodiment of the invention can be implemented using a computer program product such as, for example, a computer system 300 as shown in FIG. 8. In particular, the processes 30, 40, 50 and methods 100 and 200 can be implemented as software, or computer readable program code, 15 executing on the computer system 300.

The computer system 300 includes a processor 301, a video display 302, and input devices 303, 304. A communication input/output (I/O) signal bus 305 provides for inputs and outputs between the processor 301 and the three PTNs 20,21,22, the 20 wireless communication system 13 and the Internet 14.

The computer system 300 also includes a memory 306 that may include random access memory (RAM) and read-only memory (ROM), input/output (I/O) interfaces 71, 307, a video interface 308, and one or more storage devices generally 25 represented by in FIG. 8 with the storage device 74. The memory 306 can be used to store the transaction code or the identification code when processing a transaction. A common bus 309 links elements of the computer system 300 to provide data transfers when processing data for transactions.

30 The video interface 308 is connected to the video display 302 and provides video signals from the computer system 300 for display on the video display 302.



User input to operate the computer system 300 can be provided by one or more of the input devices 303,304 via the I/O interface 307. For example, a user of the computer system 300 can use a keyboard as the input device 303 and/or a pointing device such as a mouse as the input device 74. The keyboard and the mouse provide input to the  
5 computer system 300. The storage device 74 can consist of one or more of the following: a floppy disk, a hard disk drive, a magneto-optical disk drive, CD-ROM, magnetic tape or any other of a number of non-volatile storage devices well known to those skilled in the art. Each of the elements in the computer system 300 is typically connected to other devices via a bus 81 that in turn can consist of data,  
10 address, and control buses.

The processes 30, 40, 50 and methods 100 and 200 are effected by instructions in the software that are carried out by the computer system 300. Again, the software may be implemented as one or more modules for implementing the  
15 method steps. That is, the system controller 11 can be a part of a computer readable program code that usually performs a particular function or related functions.

In particular, the software may be stored in a computer readable medium, including the storage device 74. The computer system 300 includes the computer  
20 readable medium having such software or program code recorded such that instructions of the software or the program code can be carried out. The use of the computer system 300 preferably effects advantageous apparatuses for validating transactions of the electronic transaction system 10.

25 The computer system 300 simply provides for illustrative purposes and other configurations can be employed without departing from the scope and spirit of the invention. The foregoing is merely exemplary of the types of computers or computer systems with which the embodiments of the invention may be practised. Typically, the processes 30, 40, 50 and methods 100 and 200 of the embodiments are resident as  
30 software or a computer readable program code recorded on a hard disk drive (generally depicted as the storage device 74) as the computer readable medium, and



read and controlled using the system controller 11. Intermediate storage of the program code and media content data and any data fetched from the network may be accomplished using the memory 306, possibly in concert with the storage device 74.

5           In some instances, the program may be supplied to the user encoded on a CD-ROM or a floppy disk (both generally depicted by the storage device 74), or alternatively could be read by the user from the network via a modem device connected to the computer system 300. Still further, the computer system 300 can load the software from other computer readable media. This may include magnetic  
10 tape, a ROM or integrated circuit, a magneto-optical disk, a radio or infra-red transmission channel between the computer and another device, a computer readable card such as a PCMCIA card, and the Internet and Intranets including email transmissions and information recorded on Internet sites and the like. The foregoing is merely exemplary of relevant computer readable media. Other computer readable  
15 media may be practised without departing from the scope and spirit of the invention.

          The electronic transaction system 10 as described in the above preferred embodiment of the invention advantageously overcomes or at least alleviates the disadvantages of conventional electronic transaction systems for validating a  
20 transaction.

          In the foregoing description, an electronic transaction system, a method and a computer program product for validating electronic transactions of users of the electronic transaction system are described. Although a preferred embodiment is  
25 described, it shall be apparent to one skilled in the art in view of this preferred embodiment that numerous changes and/or modifications can be made without departing from the scope and spirit of the invention.

**Claims:**

1. An electronic transaction system for validating a transaction of a user of said electronic transaction system, said electronic transaction system having a system controller, includes:

5

means for receiving, by said system controller of said electronic transaction system, transaction information and user information from a transaction device coupled to said system controller, said transaction information and said user information being respectively associated with said transaction and said user;

10

means for receiving, by said system controller from a wireless portable communication device associated with said user, at least one identification code associated with said wireless portable communication device;

15

means for verifying, by said a system controller, said at least one identification code and said user information based upon registered information of said user, said registered information being stored in association with said system controller;

20

and

means for determining, by said controller, whether to validate said transaction in response to said verifying.

25

2. The electronic transaction system as claimed in Claim 1, and further including means for invalidating said transaction when either said at least one identification code or said user information is not verified.
- 30 3. The electronic transaction system as claimed in Claim 1, wherein said determining means includes means for checking credit information of said

user, said credit information being stored in association with said system controller.

4. The electronic transaction system as claimed in Claim 3, and further  
5 including means for validating said transaction based upon said checking.
5. The electronic transaction system as claimed in Claim 4, and further  
including means for transmitting at least one message to said wireless  
portable communication device upon validating said transaction.
- 10 6. The electronic transaction system as claimed in Claim 1, wherein said means  
for receiving said transaction information and said user information includes  
means for prompting said user to provide at least one input to obtain at least  
some of said user information.
- 15

7. An electronic transaction system for validating a transaction of a user of said electronic transaction system, said electronic transaction system having a system controller, includes:

5 means for receiving, by said system controller of said electronic transaction system, transaction information and user information from a transaction device coupled to said system controller, said transaction information and said user information being respectively associated with said transaction and said user;

10

means for transmitting, by said system controller to a wireless portable communication device associated with said user, at least one transaction code associated with said transaction;

15 means for receiving, by said system controller via said transaction device, said at least one transaction code for verification;

and

20 means for determining, by said system controller, whether to validate said transaction based upon said verification.

— 8. The electronic transaction system as claimed in Claim 7, and further including means for invalidating said transaction when said verification of  
25 said at least one transaction code fails.

9. The electronic transaction system as claimed in Claim 7, wherein said determining means includes means for checking credit information of said user, said credit information being stored in association with said system  
30 controller.

10. The electronic transaction system as claimed in Claim 9, and further including means for validating said transaction based upon said checking.
- 5 11. The electronic transaction system as claimed in Claim 10, and further including means for transmitting at least one message to said wireless portable communication device upon validating said transaction.
- 10 12. The electronic transaction system as claimed in Claim 7, wherein said means for receiving said transaction information and said user information includes means for prompting said user to provide at least one input to obtain at least some of said user information.

13. A method for validating a transaction of a user of an electronic transaction system, said method including the steps of:

receiving, by a system controller of said electronic transaction system,  
transaction information and user information from a transaction device  
coupled to said system controller, said transaction information and said user  
information being respectively associated with said transaction and said user;

receiving, by said system controller from a wireless portable  
communication device associated with said user, at least one identification  
code associated with said wireless portable communication device;

verifying, by said a system controller, said at least one identification code  
and said user information based upon registered information of said user, said  
registered information being stored in association with said system controller;

and

determining, by said system controller, whether to validate said  
transaction based upon said verifying step.

14. The method as claimed in Claim 13, and further including the step of  
invalidating said transaction when either said at least one identification code  
or said user information is not verified.

15. The method as claimed in Claim 13, wherein said determining step includes  
the step of checking credit information of said user, said credit information  
being stored in association with said system controller.

16. The method as claimed in Claim 15, and further including the step of  
validating said transaction based upon said checking step.



17. The method as claimed in Claim 16, and further including the step of transmitting at least one message to said wireless portable communication device upon validating said transaction.
- 5
18. The method as claimed in Claim 13, wherein said step of receiving said transaction information and said user information includes the step of prompting said user to provide at least one input to obtain at least some of said user information.
- 10

19. A method for validating a transaction of a user of an electronic transaction system, said method including the steps of:

receiving, by a system controller of said electronic transaction system,  
transaction information and user information from a transaction device  
coupled to said system controller, said transaction information and said user  
information being respectively associated with said transaction and said user;

transmitting, by said system controller to a wireless portable  
communication device associated with said user, at least one transaction code  
associated with said transaction;

receiving, by said system controller via said transaction device, said at  
least one transaction code for verification;

and

determining, by said system controller, whether to validate said  
transaction based upon said verification.

20. The method as claimed in Claim 19, and further including the step of  
invalidating said transaction when said verification of said at least  
one transaction code fails.

21. The method as claimed in Claim 19, wherein said determining step includes  
the step of checking credit information of said user, said credit information  
being stored in association with said system controller.

22. The method as claimed in Claim 21, and further including the step of  
validating said transaction based upon said checking step.

23. The method as claimed in Claim 22, and further including the step of transmitting at least one message to said wireless portable communication device upon validating said transaction.
- 5 24. The method as claimed in Claim 19, wherein said step of receiving said transaction information and said user information includes the step of prompting said user to provide at least one input to obtain at least some of said user information.

25. A computer program product with a computer usable medium having a computer readable program code means embodied therein for validating a transaction of a user of an electronic transaction system having a system controller, said computer program product including:

5

computer readable program code means for receiving, by said system controller of said electronic transaction system, transaction information and user information from a transaction device coupled to said system controller, said transaction information and said user information being respectively associated with said transaction and said user;

10

computer readable program code means for receiving, by said system controller from a wireless portable communication device associated with said user, at least one identification code associated with said wireless portable communication device;

15

computer readable program code means for verifying, by said system controller, said at least one identification code and said user information based upon registered information of said user, said registered information being stored in association with said system controller;

20

and

computer readable program code means for determining, by said controller, whether to validate said transaction in response to said verifying.

25

26. The computer program product as claimed in Claim 25, and further including computer readable program code means for invalidating said transaction when either said at least one identification code or said user information is not verified.

30

27. The computer program product as claimed in Claim 25, wherein said computer readable program code means for determining includes computer readable program code means for checking credit information of said user, said credit information being stored in association with said system controller.
28. The computer program product as claimed in Claim 27, and further including computer readable program code means for validating said transaction based upon said checking.
29. The computer program product as claimed in Claim 28, and further including computer readable program code means for transmitting at least one message to said wireless portable communication device upon validating said transaction.
30. The computer program product as claimed in Claim 25, wherein said computer readable program code means for receiving said transaction information and said user information includes computer readable program code means for prompting said user to provide at least one input to obtain at least some of said user information.

31. A computer program product with a computer usable medium having a computer readable program code means embodied therein for validating a transaction of a user of an electronic transaction system having a system controller, said computer program product including:

5

computer readable program code means for receiving, by said system controller of said electronic transaction system, transaction information and user information from a transaction device coupled to said system controller, said transaction information and said user information being respectively associated with said transaction and said user;

10

computer readable program code means for transmitting, by said system controller to a wireless portable communication device associated with said user, at least one transaction code associated with said transaction;

15

computer readable program code means for receiving, by said system controller via said transaction device, said at least one transaction code for verification;

20

and

computer readable program code means for determining, by said controller, whether to validate said transaction based upon said verification.

- 25 32. The computer program product as claimed in Claim 31, and further including computer readable program code means for invalidating said transaction when said verification of said at least one transaction code fails.

- 30 33. The computer program product as claimed in Claim 31, wherein said computer readable program code means for determining includes computer readable program code means for checking credit information of said user,



said credit information being stored in association with said system controller.

- 5 34. The computer program product as claimed in Claim 33, and further including computer readable program code means for validating said transaction based upon said checking.
- 10 35. The computer program product as claimed in Claim 34, and further including computer readable program code means for transmitting at least one message to said wireless portable communication device upon validating said transaction.
- 15 36. The computer program product as claimed in Claim 31, wherein said computer readable program code means for receiving said transaction information and said user information includes computer readable program code means for prompting said user to provide at least one input to obtain at least some of said user information.

-1/13-

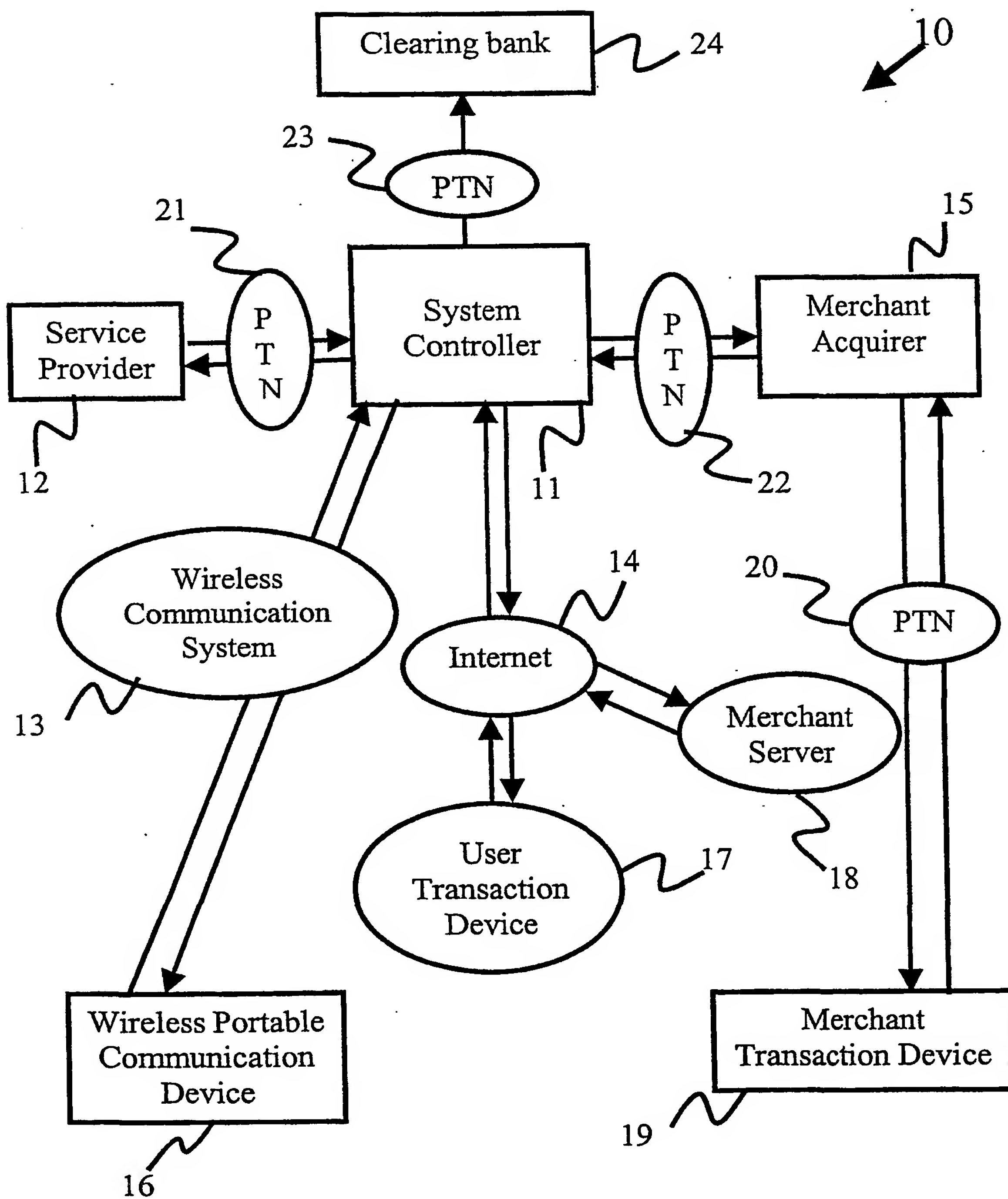


FIG. 1

-2/13-

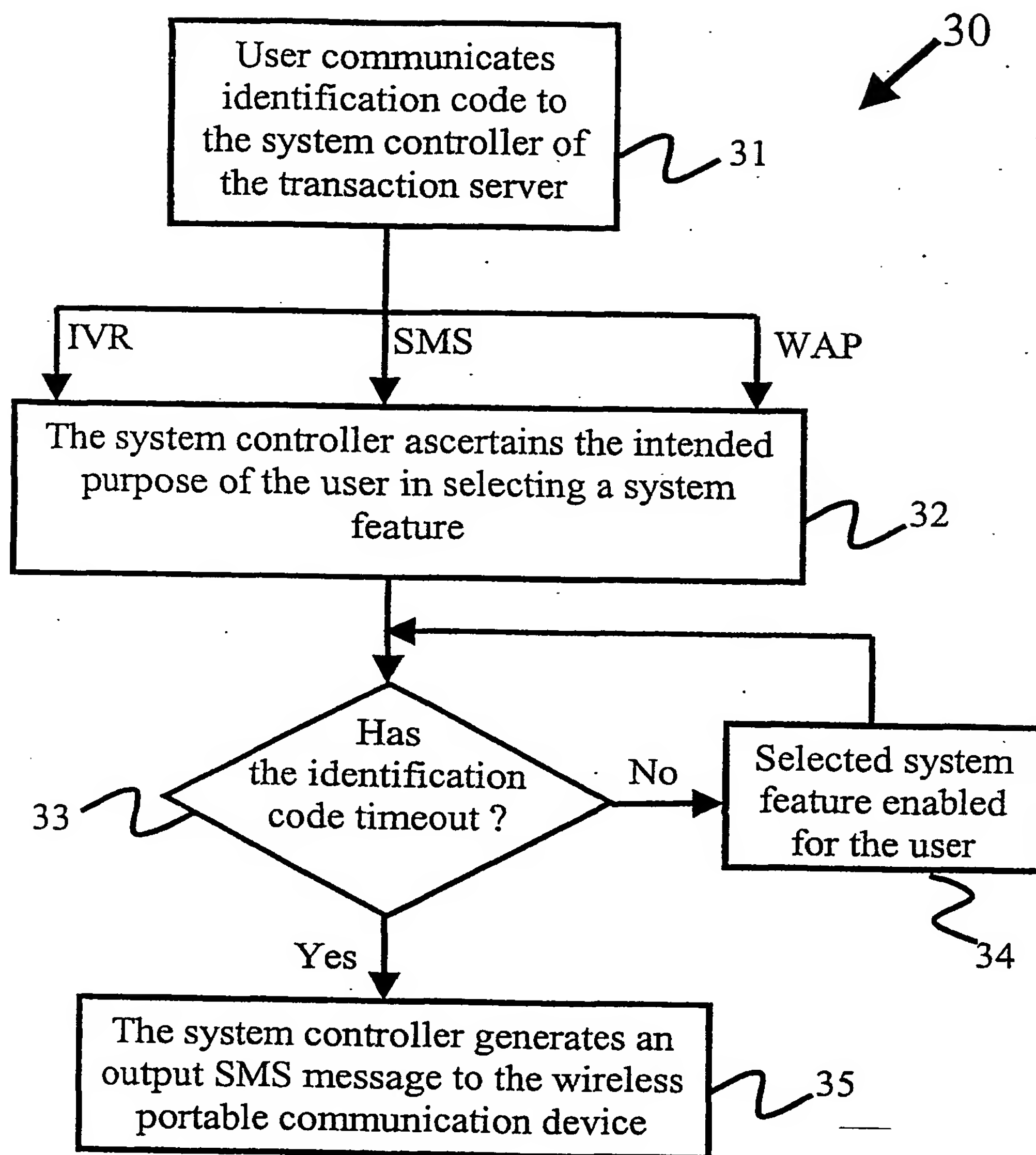


FIG. 2

-3/13-

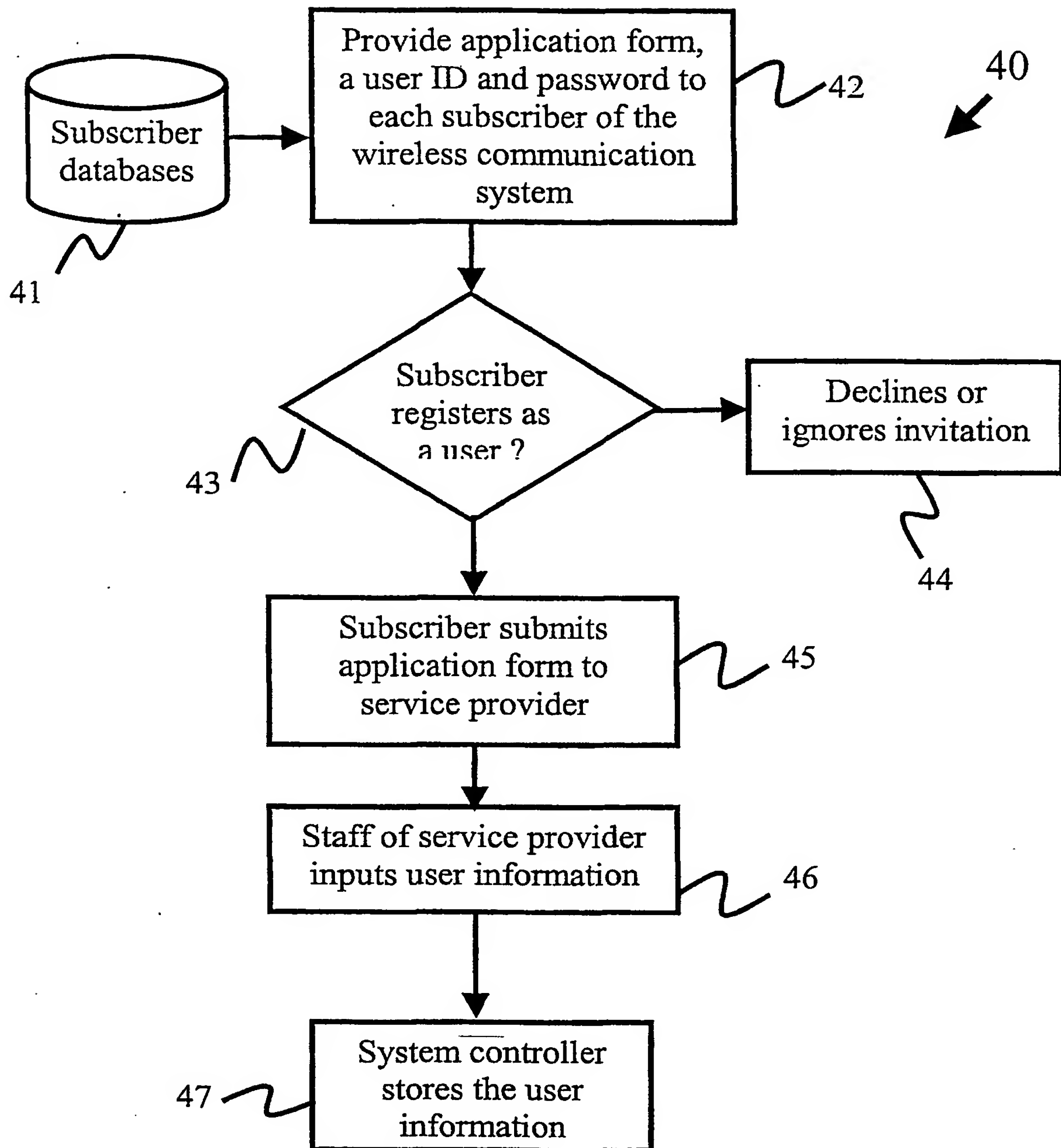


FIG. 3

-4/13-

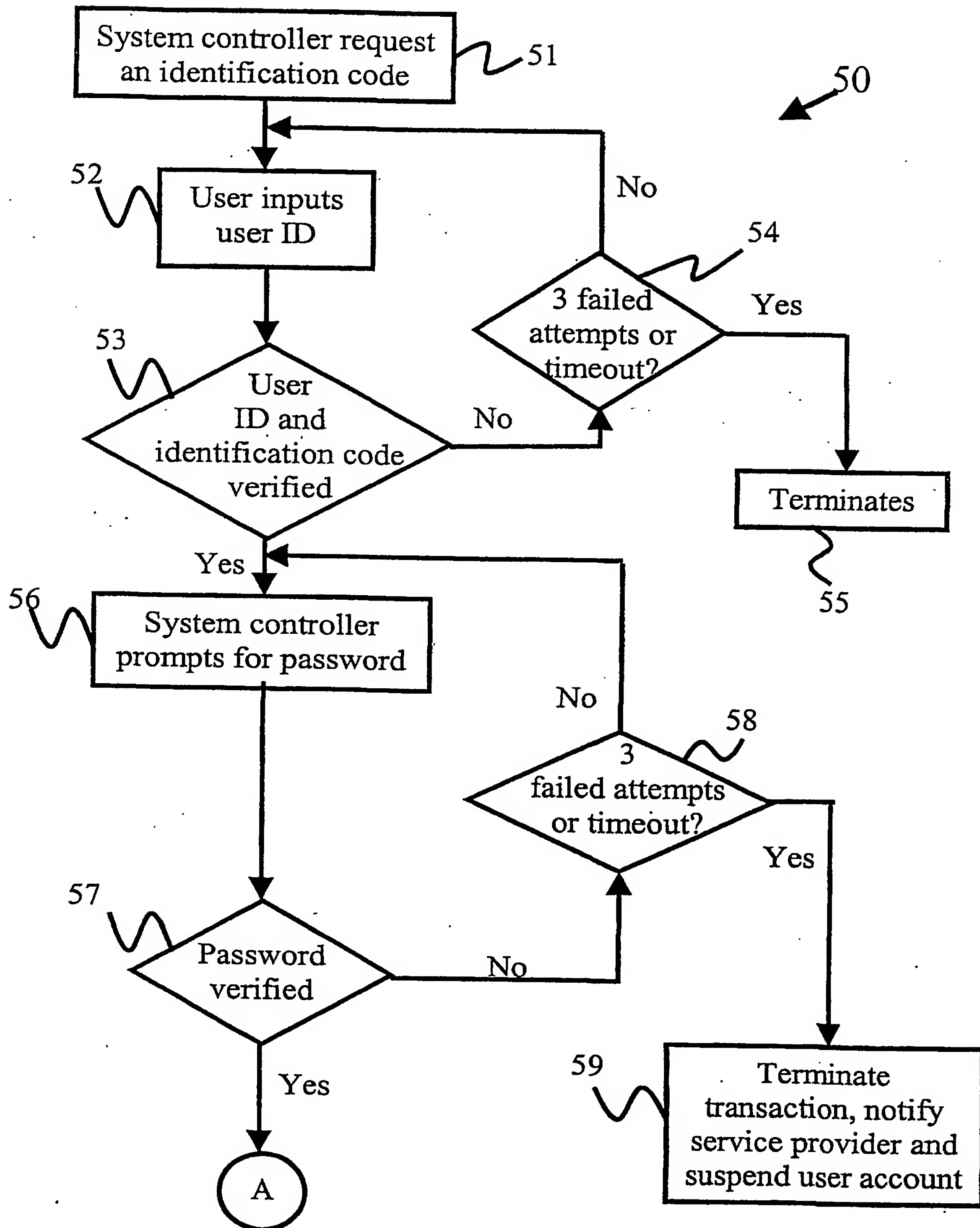


FIG. 4a

-5/13-

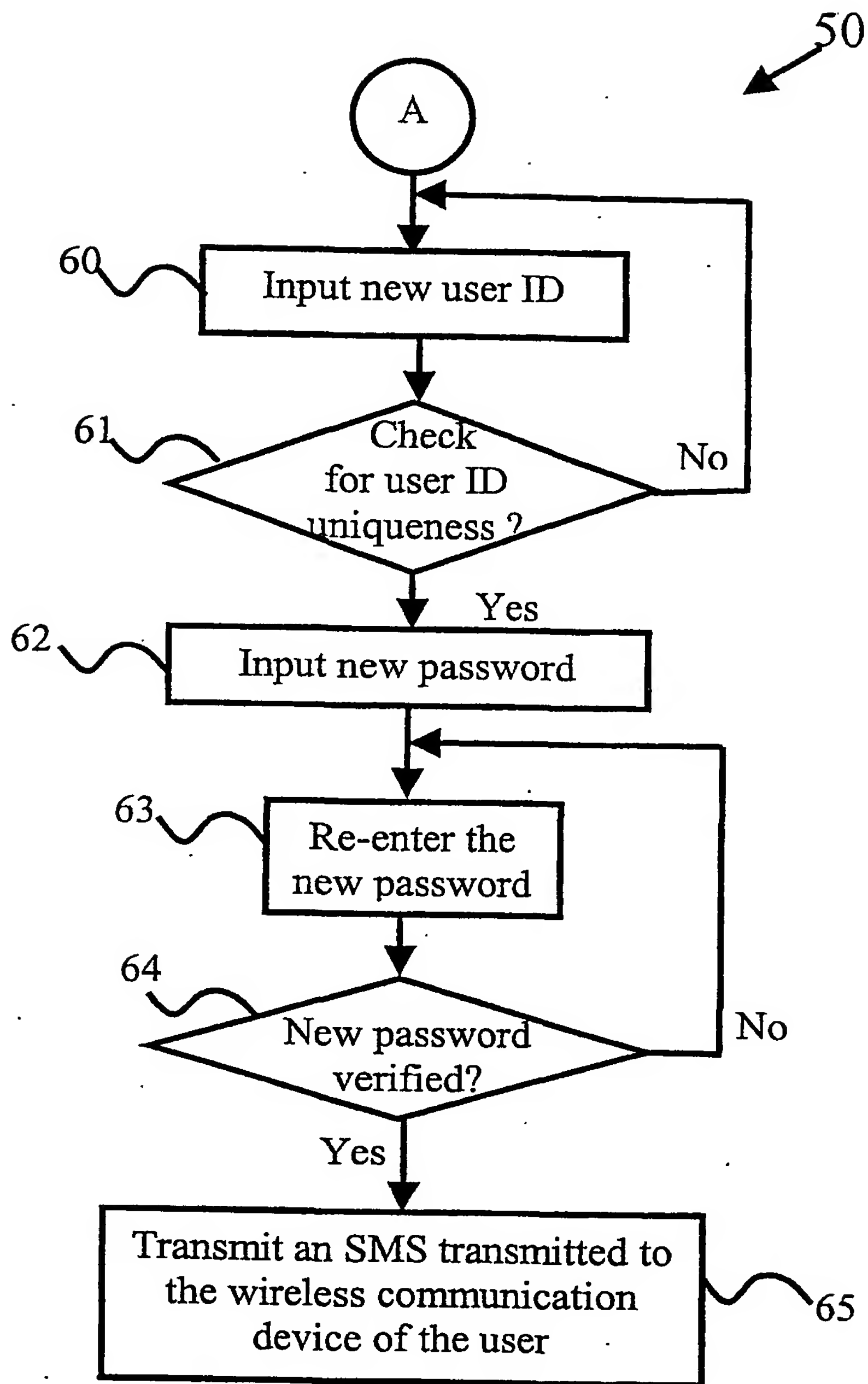


FIG. 4b



-6/13-

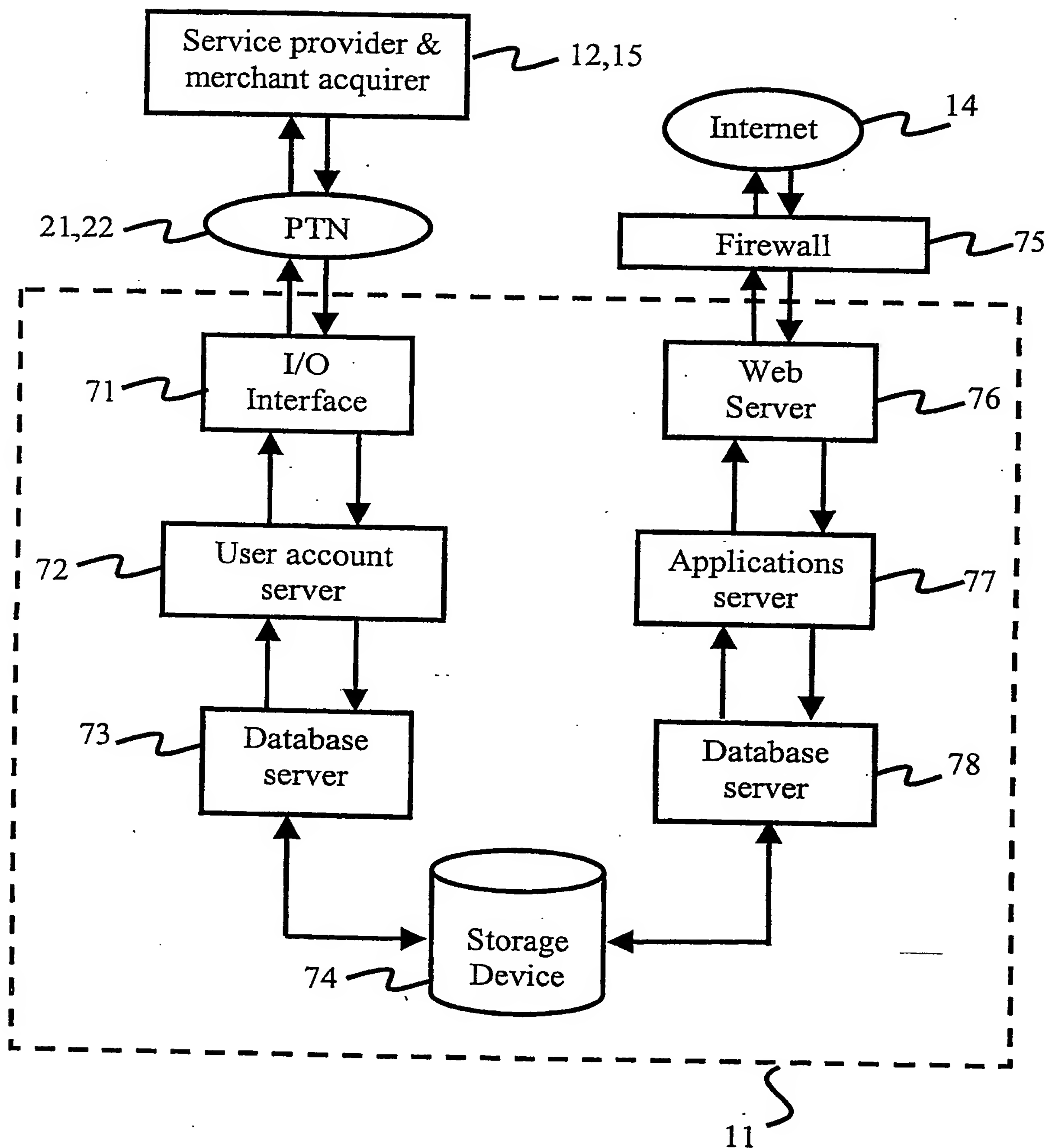


FIG. 5

-7/13-

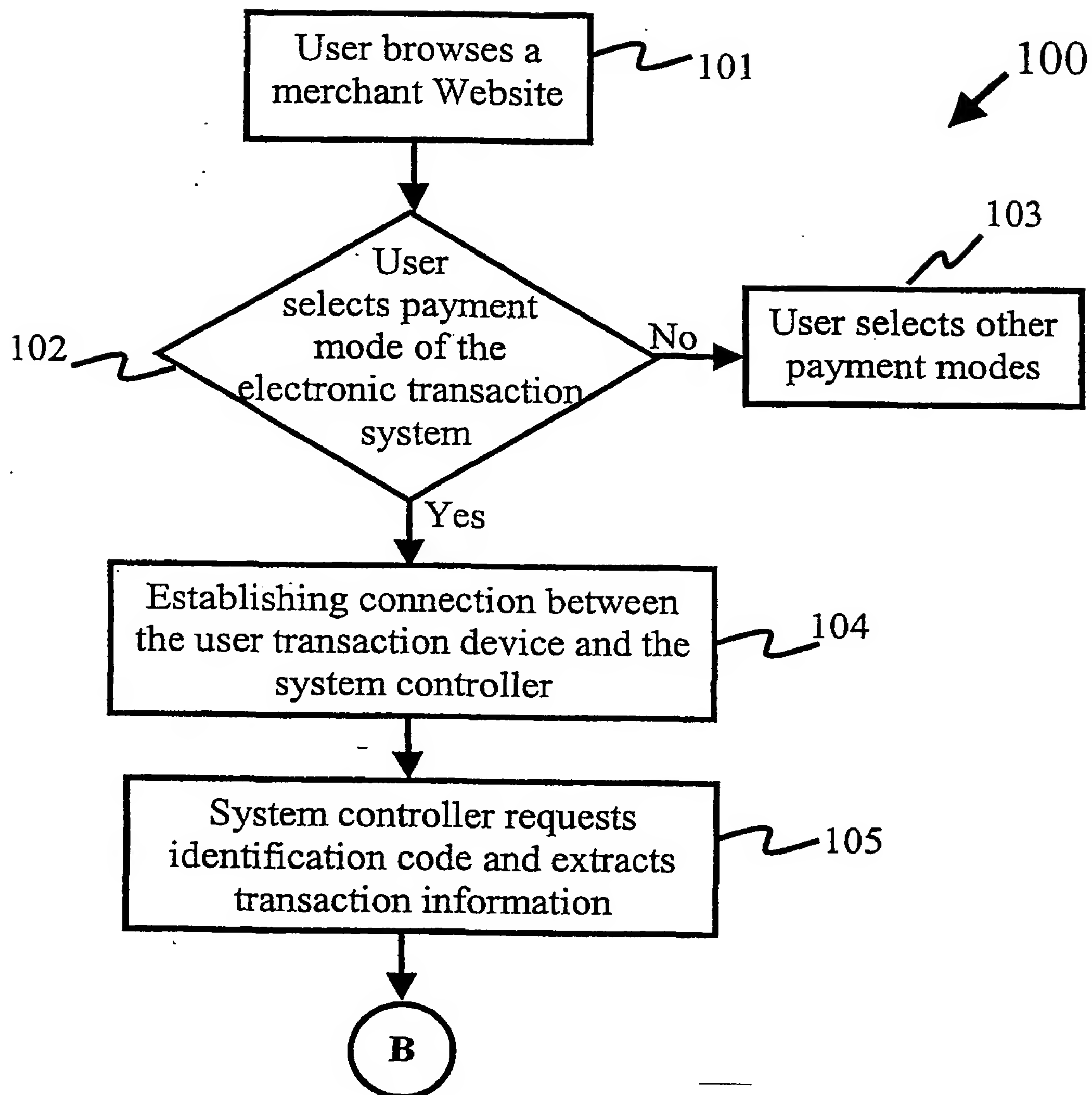


FIG. 6a

-8/13-

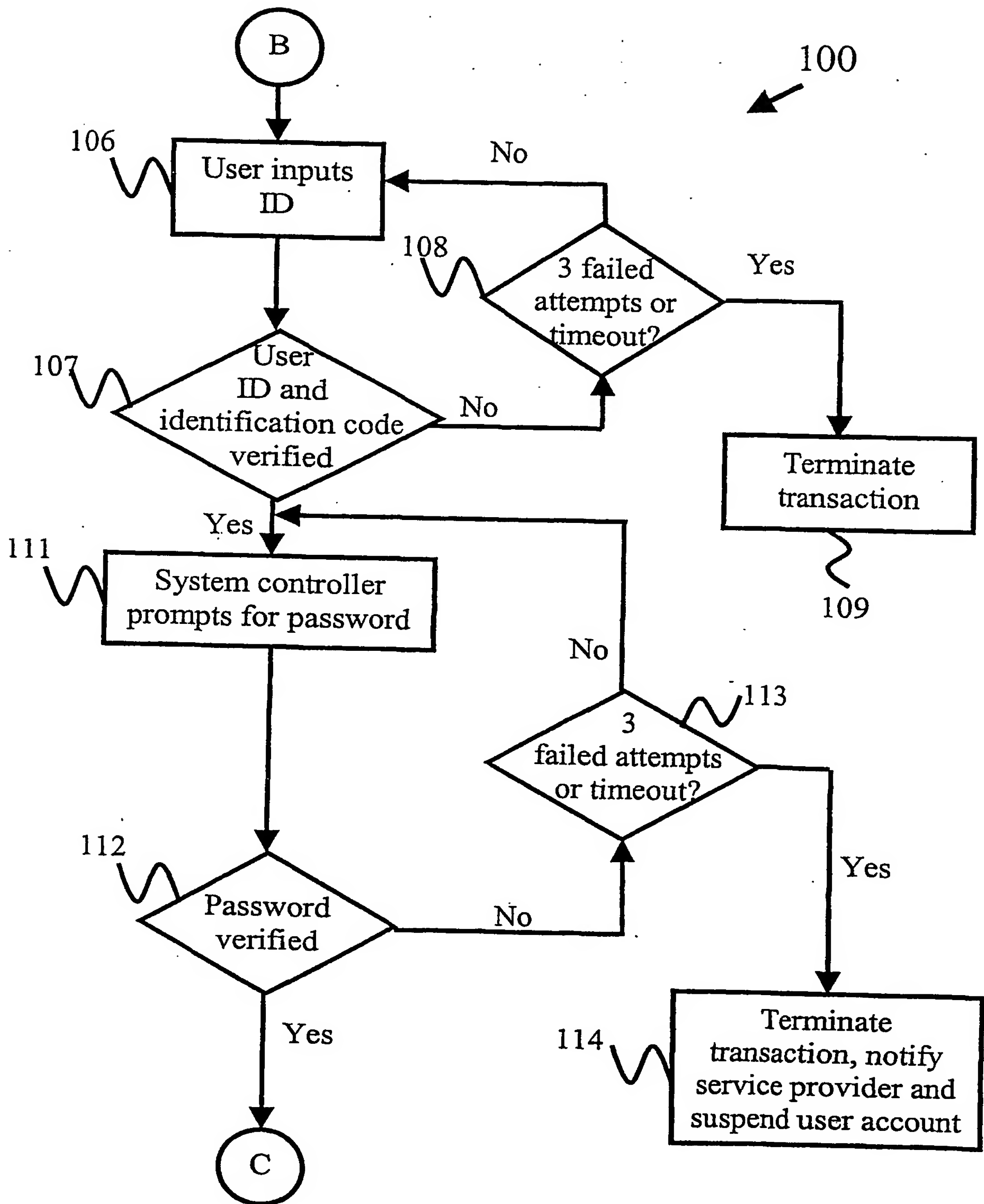


FIG. 6b

-9/13-

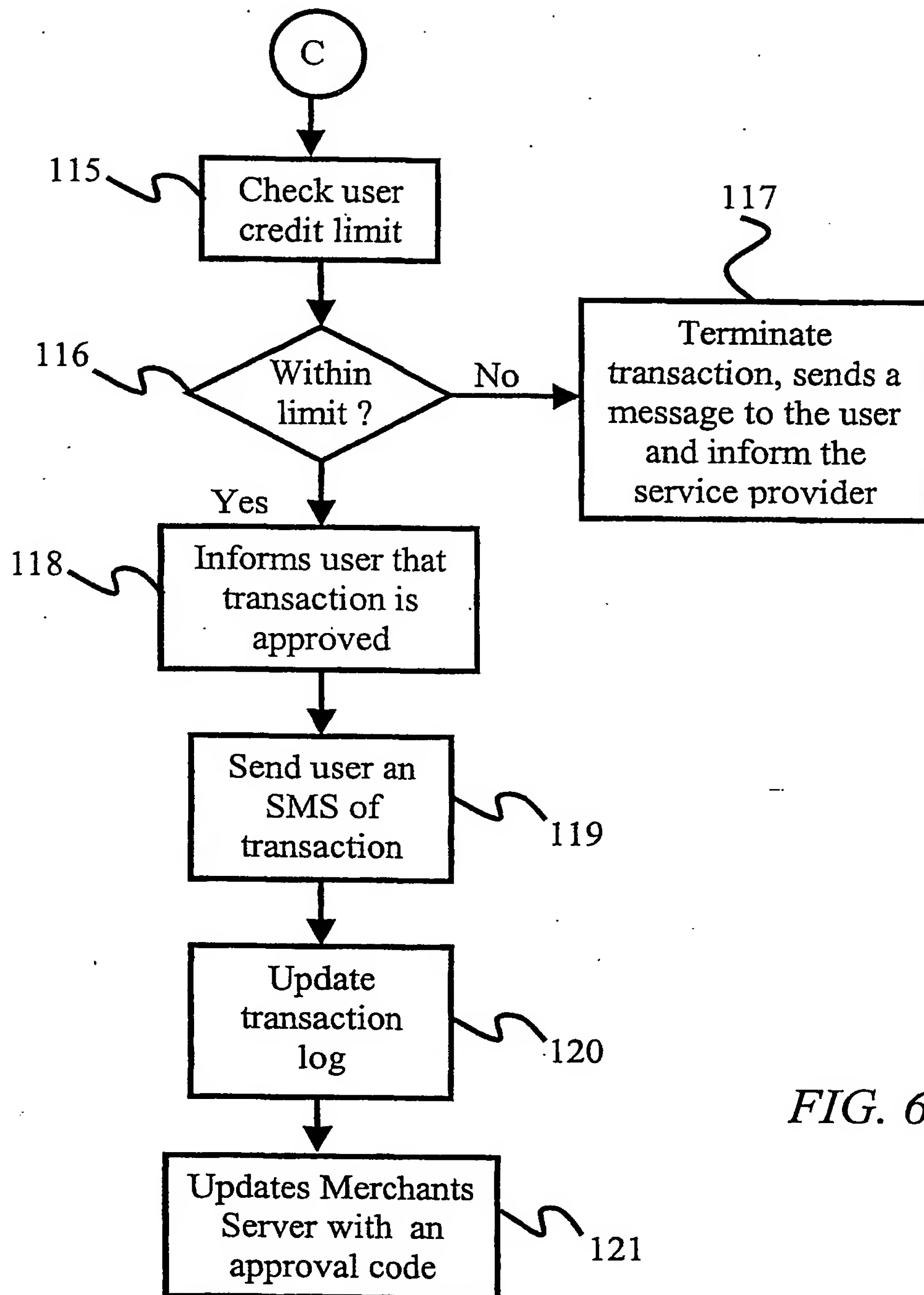


FIG. 6c

-10/13-

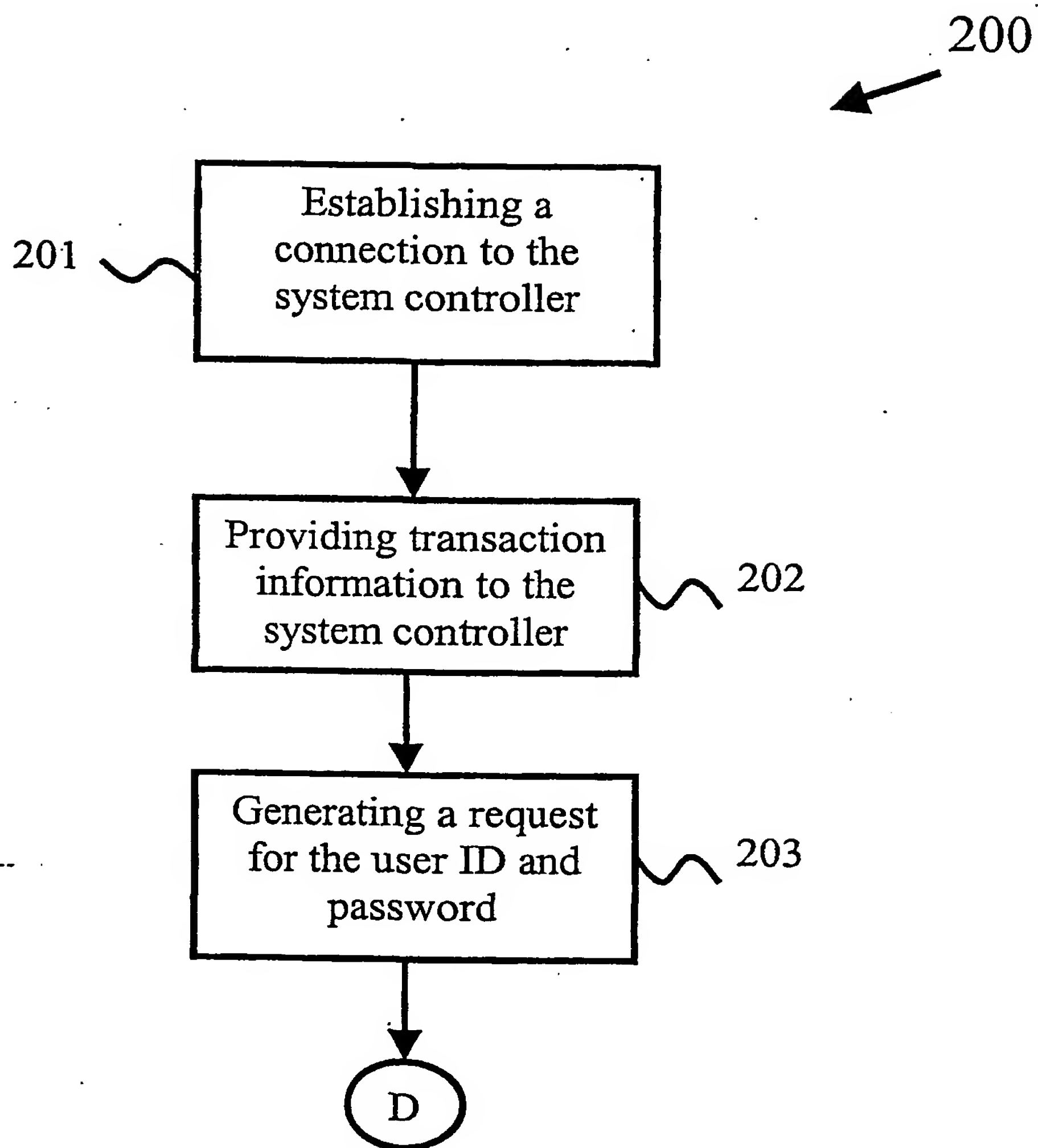


FIG. 7a

-11/13-

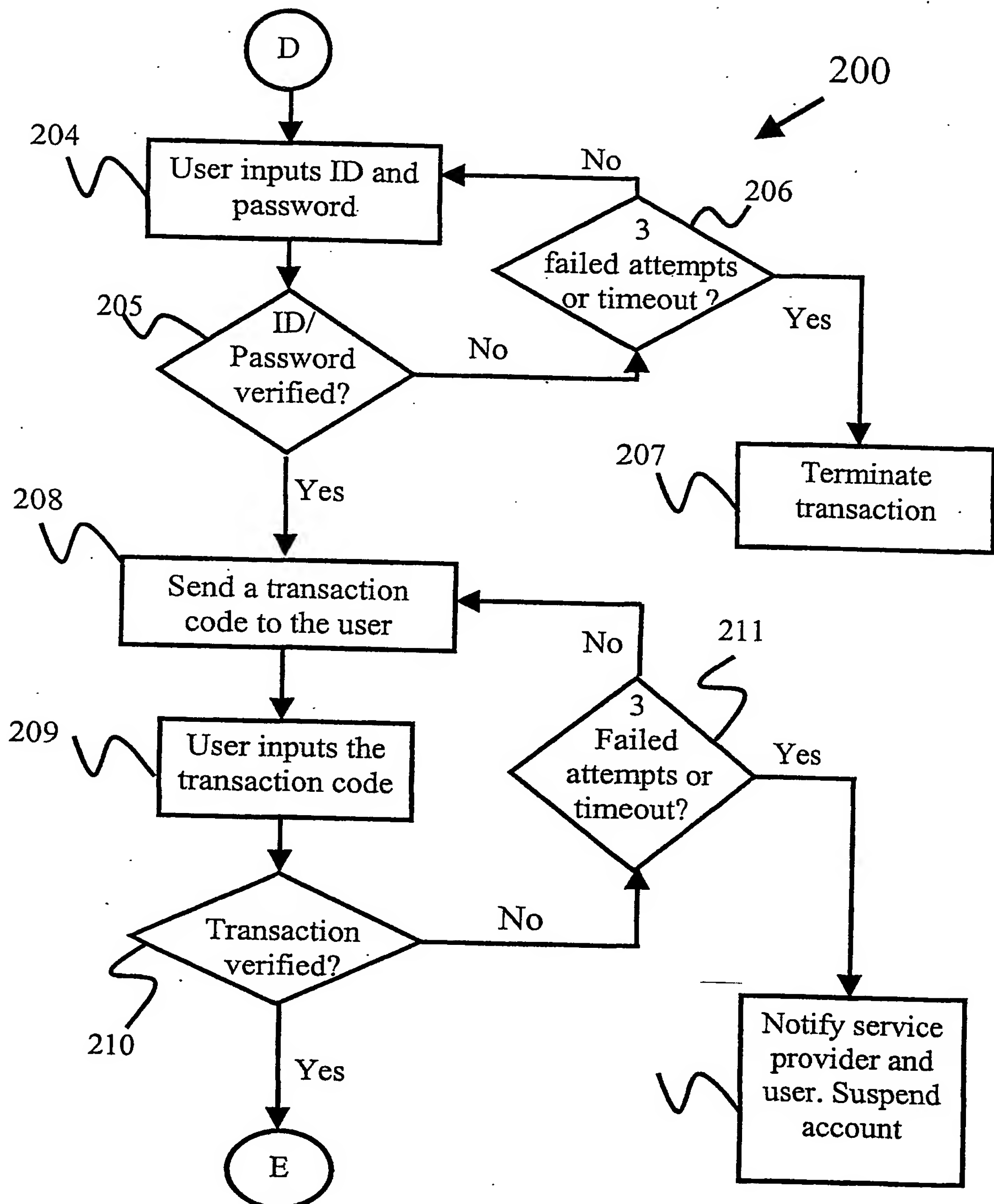
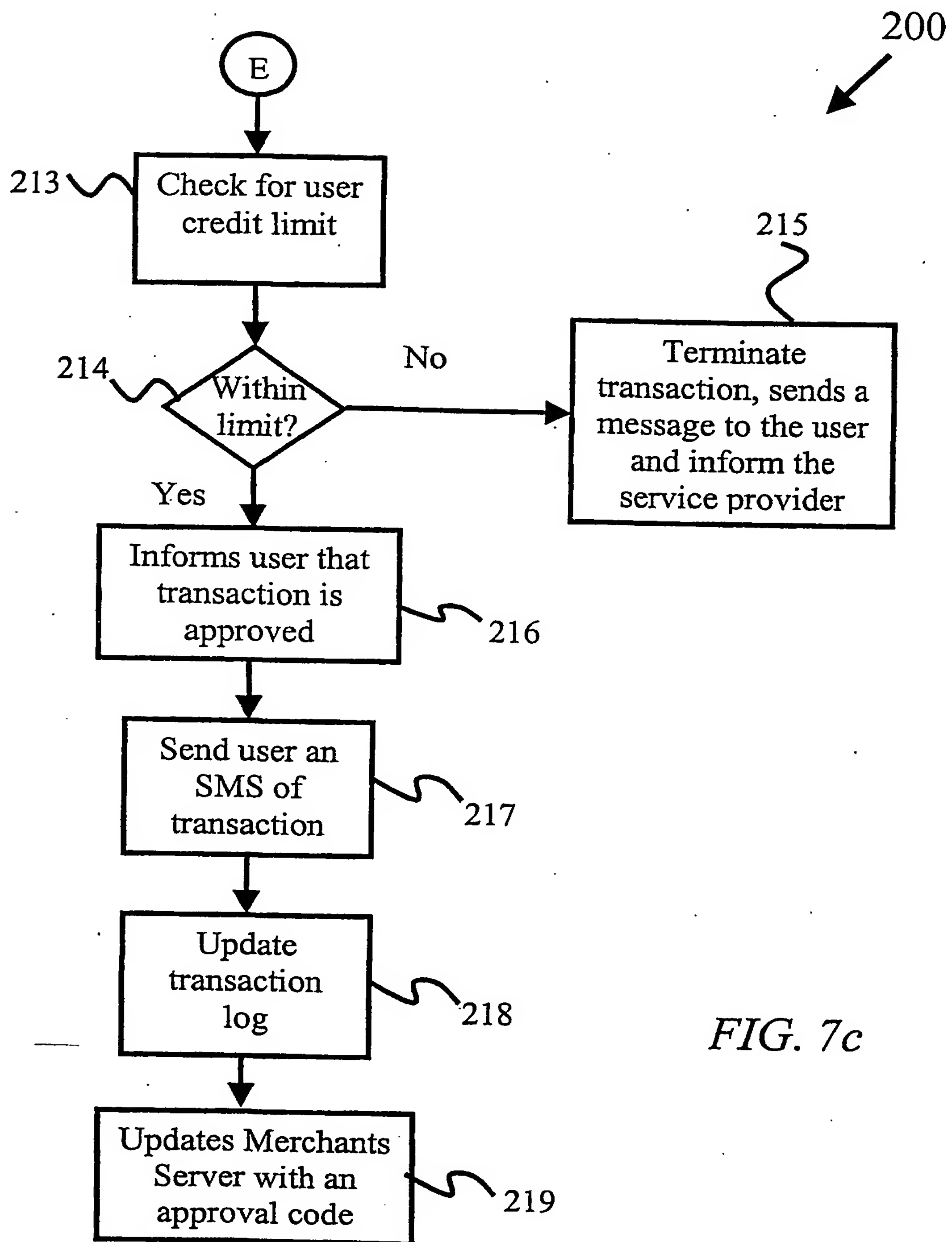


FIG. 7b



-12/13-



-13/13-

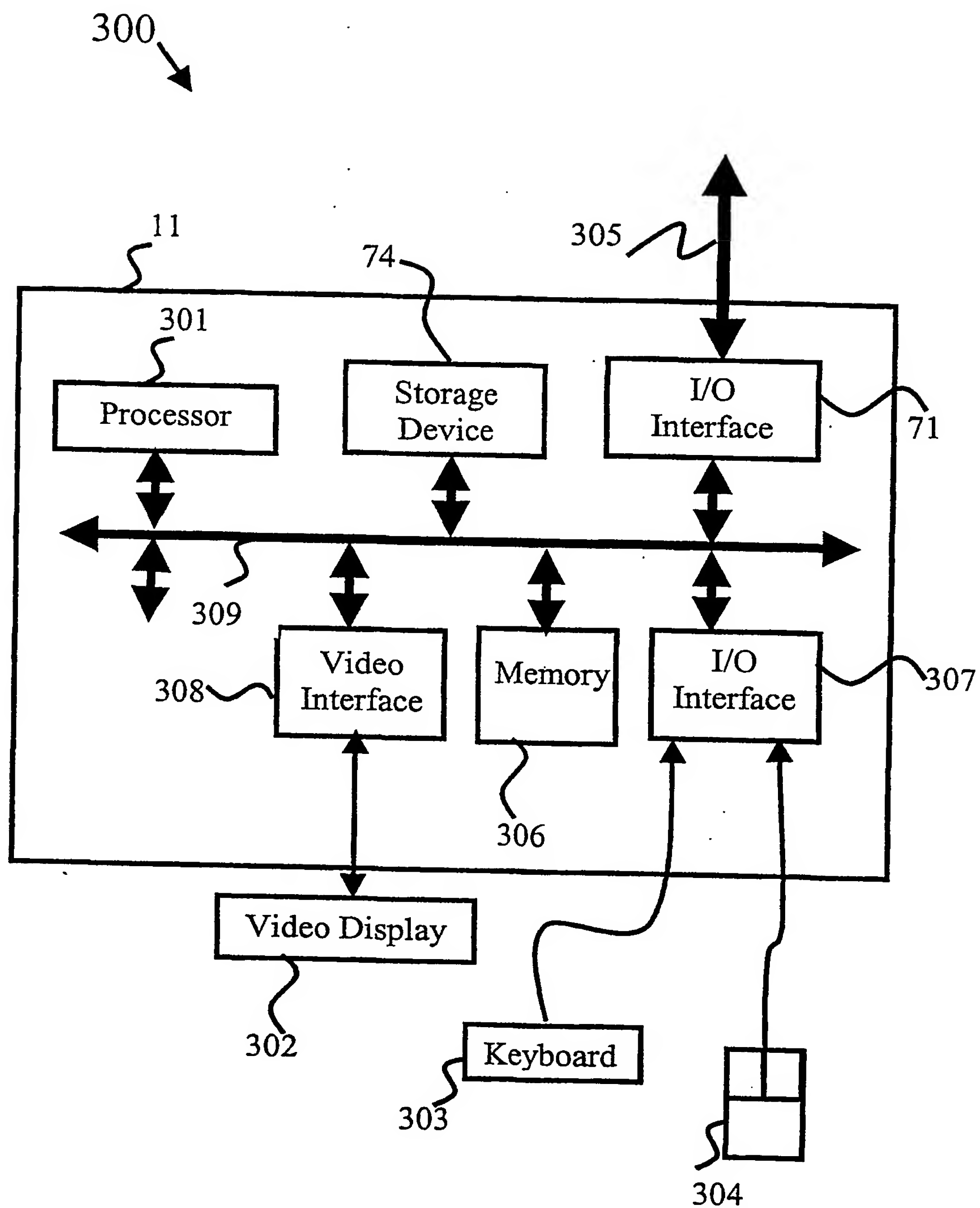


FIG. 8

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/SG00/00180

**A. CLASSIFICATION OF SUBJECT MATTER**Int. Cl. <sup>7</sup>: G06F 17/60

According to International Patent Classification (IPC) or to both national classification and IPC

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)

IPC: G06F 17/60, H04Q/IC, G07F 19/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

AU: IPC AS ABOVE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPAT: MOBILE OR PORTABLE OR CELL; PHONE? OR TELEPHONE? OR DEVICE?; +COMMERCE  
OR EFTPOS OR TRANSACT+; PURCHASE+ OR BUY+ OR SHOP+; VENDOR? OR  
MERCHANT? OR SELLER?; IDENTIF+ OR VERIF+ OR VALIDAT+ OR "ID"; CODE?**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, Y	EP 367361 A (GTE MOBILNET INCORPORATED) 9 May 1990 Entire document	1-36
X	US 6039247 A (RECCIA et al.) 21 March 2000 Entire document - particularly abstract, columns 1 & 2, drawings	1-24
Y	Entire document - particularly abstract, columns 1 & 2, drawings	25-36
X	WO 97/45814 A (VAZVAN) 4 December 1997 Entire document	1-24
Y	Entire document	25-36

☒ Further documents are listed in the continuation of Box C ☒ See patent family annex

## \* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

28 February 2001

Date of mailing of the international search report

5 March 2001

Name and mailing address of the ISA/AU

AUSTRALIAN PATENT OFFICE  
PO BOX 200, WODEN ACT 2606, AUSTRALIA  
E-mail address: pct@ipaaustralia.gov.au  
Facsimile No. (02) 6285 3929

Authorized officer

CHARLES BERKO

Telephone No : (02) 6283 2169

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/SG00/00180

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WO 94/11849 A (VATANEN) 26 May 1994 Entire document - particularly page 6 paragraph 1 Entire document	1-24 25-36
X A	WO 98/37524 A (SWISSCOM AG) 27 August 1998 Entire document - particularly abstract, drawings	1-24 25-36
X A	EP 848360 A (BRITISH TELECOMUNICATIONS public limited company) 17 June 1998 Entire document	1-24 25-36
X Y	GB 2319381 A (EASTMAR HOLDINGS LIMITED) 20 May 1998 Entire document - particularly page 3 Entire document	1-24 25-36
X, Y	WO 98/47116 A (TELEFONAKTIEBOLAGET LM ERICSSON) 22 October 1998 Entire document	1-36
Y	WO 98/35521 A (TELEFONAKTIEBOLAGET LM ERICSSON) 13 August 1998 Entire document	1-36

INTERNATIONAL SEARCH REPORT  
Information on patent family members

International application No.  
PCT/SG00/00180

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member			
EP	367361	CA	2001857	US	4958368
US	6039247	NONE			
WO	9745814	EP	960402	FI	971009
		FI	962553	FI	971248
		FI	945075	FI	962961
		WO	9613814	WO	9719568
WO	9411849	EP	669031	FI	925135
		NO	951814	FI	934995
WO	9837524	AU	60868/98	AU	80070/98
		EP	993664	NO	996147
EP	848360	NONE			
GB	2319381	IE	71908 B3		
WO	9847116	AU	70943/98	BR	9808534
		NO	995031	EP	976116
WO	9835521	AU	60084/98	US	6081705
END OF ANNEX					

